UNIVERSITÉ DE LIMOGES
ÉCOLE DOCTORALE SCIENCES ET INGÉNIERIE POUR L'INFORMATION, MATHÉMATIQUES
FACULTÉ DES SCIENCES ET TECHNIQUES
ET
UNIVERSITÉ MOHAMMED V DE RABAT
FACULTÉ DES SCIENCES

THÈSE DE DOCTORAT

Présentée par
Nora EL AMRANI

Discipline : **Mathématiques et Applications**
Spécialité : **Codes correcteurs d'erreurs et cryptographie**

CODES ADDITIFS ET MATRICES MDS POUR LA CRYPTOGRAPHIE

Soutenue le : Le **24 Février 2016**
Devant le jury

Président

Said EL HAJJI	Professeur, Université Mohammed V, Rabat.

Examinateurs :

Marine MINIER	Maître de Conférences HDR, INSA de Lyon.
Ayoub OTMANI	Professeur, Université de Rouen.
Abdelkader NECER	Maître de Conférences, Université de Limoges.
Pierre LOIDREAU	Ingénieur HDR, DGA et Univ. de Rennes.
Thierry P. BERGER	Professeur, Université de Limoges.
El Mamoun SOUIDI	Professeur, Université Mohammed V, Rabat.

Faculté des Sciences et Techniques, Xlim, 123 Avenue Albert Thomas, 87000 Limoges-FRANCE Tél. : 05 55 45 72 00 - Fax : 05 55 45 72 01, *http : //www.sciences.unilim.fr*
Faculté des Sciences, 4 Avenue Ibn Battouta B.P 1014 RP, Rabat-MAROC Tél +212 (0) 537 77 18 34/35/38, Fax : +212 (0) 537 77 42 61, *http : //www.fsr.ac.ma*

Dédicaces

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez.

À ***mon cher mari :***

Pour être à mes côtés malgré la distance qui nous a séparé pendant mes séjours à Limoges, pour ton soutien et ton amour inconditionnel. Pour croire en moi pendant mes périodes de doute et pour tes multiples encouragements répétés.

À ***mes très chers parents :***

Pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance, pour mon éducation et mon bien être.

Les prières de ma mère, sa bénédiction et ses conseils. Le grand coeur de mon père et ses encouragements, mon père qui a été la première personne à m'apprendre à compter et à démontrer. Et avec lequel je trouve toujours le plaisir de discuter Mathématiques.

Tout cela m'a été d'un grand secours pour mener à bien mes études. J'espère que vous trouvez dans ces mots l'expression de ma très grande considération et mon dévouement le plus sincère. Que Dieu vous garde et vous accorde longue vie.

À ***tous ceux qui me sont très chers.***

Avant Propos

Cette thèse a été réalisée en cotutelle entre l'Université de Limoges et l'Université Mohammed V de Rabat.Cette convention de cotutelle a été soutenu par la bourse volubilis de cotutelle du projet Hubert Curien MA/12/169 et par une bourse régional.

Je voudrais tout d'abord remercier le Professeur Thierry BERGER de l'Université de Limoges et le Professeur El Mamoun SOUIDI de l'Université Mohammed V de Rabat, mes directeurs de thèse qui sont à l'origine de ce travail. C'est un honneur pour moi de travailler avec eux et je ne peux qu'admirer leur talent. Je les suis infiniment reconnaissante, non seulement parce qu'ils ont accepté de me prendre en thèse, mais aussi pour le partage de leurs idées et leur savoir avec moi. Ils ont dirigé ma thèse avec beaucoup de patience et ils ont dédié beaucoup de temps à mon travail en étant toujours très disponible malgré leurs nombreuses charges. Je les remercie aussi d'avoir lu très sérieusement beaucoup de versions préliminaires de ces travaux.

Je tiens à exprimer ma profonde gratitude au Professeur Said EL HAJJI de l'Université Mohammed V de Rabat, pour son soutien, ses bons conseils, et pour avoir accepté de présider ma soutenance et se déplacer du Maroc pour le faire.

Je suis très reconnaissante à Marine Minier Maître de Conférences HDR, à l'INSA de Lyon et Ayoub Otmani Professeur à l'Université de Rouen, qui ont bien voulu établir un rapport sur ma thèse. Je les remercie pour l'intérêt qu'ils ont porté à mon travail, et pour leurs remarques qui m'ont permis de parfaire mon manuscrit, en dépit du peu de temps dont ils disposaient. Abdelkader NECER Maître de Conférences à l'Université de Limoges et Pierre LOIDREAU Ingénieur HDR à DGA et l'Université de Rennes, m'ont fait l'honneur d'accepter d'être membres de mon jury, et je les en remercie sincèrement.

Mes sincères remerciements s'adressent aussi aux différentes personnes du laboratoire LabMIA à Rabat et du Laboratoire XLIM à Limoges, avec qui j'ai eu la chance de travailler, de discuter et de partager des moments agréables.

Un GRAND MERCI à mon mari, mes parents et mes frères. Merci pour vos sacrifices, vos encouragements et votre soutien qui m'ont permis d'avancer dans mes études et de devenir qui je suis.

Je tiens à exprimer ma profonde gratitude à ma grande famille, spécialement à la famille Meskine, et à toutes celles et ceux qui m'ont apporté leur soutien, leur amitié ou leur expérience tout au long de ce travail de thèse.

Table des matières

Introduction Générale

En 1623 Francis Bacon présente dans "De dignitate et augmentis scientiarum" son alphabet appelé "alphabet bilitaire", où il a remplacé les lettres de son temps par des arrangements de taille 5 avec seulement deux lettres (A et B). Ceci est semblable au système binaire utilisé aujourd'hui, et qui permet de communiquer à distance. Ainsi est né un troisième âge de la communication, celui de la numérisation.

Bien que l'information, qui est devenue entièrement numérique, doit avant tout être transmise, assurer sa protection et son intégrité sont aussi des priorités. Ces derniers concepts sont inspectés respectivement par deux nouvelles sciences, à savoir la cryptologie et la théorie des codes correcteurs d'erreurs.

C'est en 1948, que le problème de l'intégrité de l'information transmise en présence de bruit a été soulevé par Shannon (nommé le père de la théorie des informations) dans son papier [41] intitulé "A Mathematical Theory of Information" où il a établi les concepts fondamentaux de la théorie des codes.

Lors d'envoi d'un message à travers un canal bruité, le message peut faire l'objet de quelques erreurs à la réception, par exemple à l'envoi de "1101" on peut recevoir "0101". L'idée du codage est la suivante : avant d'envoyer le message, il doit ÃŁtre coder, et par la suite il sera décodé à la réception.

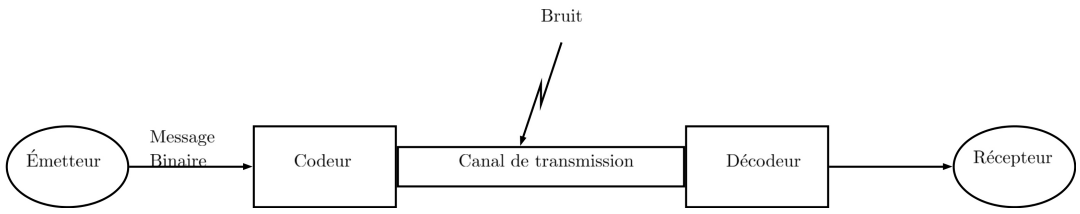

FIGURE 1 – Schéma de Claude Shannon illustrant le principe du codage

Le problème de l'intégrité de l'information ne persiste pas seulement en cas de transmission des donnés, mais aussi dans plusieurs autres circonstances, par exemple la perte d'information sur les DVD ou les CD suite à des rayures, défauts de fabrication ... est très fréquente.

Habituellement n spécifie la longueur binaire des mots du code ($n = 4$ pour l'exemple cité en dessus). La théorie des codes établie par Shannon, promet seulement l'existence de bons codes mais ne permet malheureusement pas la

détection et/ou la correction des erreurs, autrement dit elle ne propose pas de méthode de construction de codes capables d'assurer l'intégrité de l'information.
La théorie des codes correcteurs d'erreurs repose sur le principe de redondance, c'est-à-dire l'ajout de la redondance au message avant de l'envoyer. Ce principe consiste à adjoindre au message à envoyer (de taille k), un bloc de symboles de l'alphabet appelé redondance (de taille r) afin d'obtenir un message encodé de taille $n = k + r$. Cet ajout est fait à l'aide d'une fonction appelée fonction d'encodage, les mots obtenus par l'application de cette fonction aux messages sont appelés mots du code. Le codage permet de constater s'il y a eu un éventuel changement (ajout de bruit) dans le message envoyé en vérifiant l'appartenance du mot reçu à l'ensemble des mots du code.
Depuis l'énoncé de Shannon sur les codes, construire de bons codes, autrement dit des codes capables de détecter et/ou de corriger le maximum d'erreurs, fascine les chercheurs du monde entier. Les principaux objectifs que la théorie des codes correcteurs d'erreurs cherche à atteindre sont les suivants :

— maximiser la quantité de l'information transmise par unité de temps.
— maximiser la détection des erreurs et la capacité de correction.
— permettre une transmission rapide de l'information codée.
— réaliser un codage rapide.
— réaliser un décodage rapide.

Les deux premiers objectifs font aujourd'hui la priorité des mathématiciens.

Un des exemples simples d'un code correcteur est celui des codes de parité. Reprenant l'exemple du message 1101, si on ajoute une redondance de parité (la somme de tous les symboles du mot), le résultat de son encodage donne le mot 11011. Un deuxième exemple basique est celui des codes à répétition : on répète le message un certain nombre de fois avant de l'envoyer, par exemple une répétition de 3 fois donne le mot : 110111011101, pour décoder à la réception, on compte combien de fois chaque chaîne de longueur k (dans ce cas $k = 4$) se répète, et la chaîne qui se répète le plus de fois, c'est le message. Ces deux exemples montrent que l'augmentation de la taille du message (la redondance) permet de détecter des erreurs mais au détriment de la réduction de la vitesse de transmission. Cela éclaire la contradiction entre les deux principaux buts de la théorie des codes et fait la difficulté de leur construction.

En ce qui concerne la cryptologie, son existence date d'une époque reculée (100 av. J.-C. par Jule César). Elle englobe deux sciences, la première est la cryptographie, qui comporte l'ensemble des techniques permettant de chiffrer un message clair (le rendre illisible par un tiers) et de mettre en sûreté : sa confidentialité, son authentification, son intégrité, ainsi que sa non répudiation. La deuxième est la cryptanalyse, qui vise à attaquer ces points de sécurité.
Les deux grands volets de cryptographie sont :

— la cryptographie asymétrique [17] (à clé publique). Elle se base sur l'existence de fonctions dites à sens unique (fonctions qu'on peut facilement calculer, mais difficile à inverser) et d'une clé secrète pour déchiffrer.

— La cryptographie symétrique (à clé secrète). Elle englobe deux grandes familles qui sont : les chiffrements par flot, tel que les données sont traitées en flux, bit par bit, et le chiffrement par blocs tel que les données sont découpées en blocs (64, 128 ou 256 bits) avant d'être chiffrées. Ce chiffrement est en général constitué d'une succession de ces trois opérations : la substitution, la permutation et le XOR bit à bit avec la clé. Cette architecture est appelée un réseau de substitution et permutation, SPN (Substitution Permutation Network en Anglais).

L'alliance entre ces deux grandes sciences de sécurité de l'information, a donné naissance aux premiers cryptosystèmes à clé publique basés sur la théorie des codes, qui sont le cryptosystème de McEliece [30] en 1978, et le cryptosystème de Niederreiter [31] en 1986. En revanche la grande taille des clés est le plus grand des inconvénients de ces deux cryptosystèmes. En cryptographie symétrique, *AES* [16] est le plus connu des cryptosystèmes basés sur un réseau SPN, dont la matrice MixColumns assure la bonne diffusion. Cette matrice a de bonnes propriétés de diffusion et est en fait directement relié à un code MDS (Maximum Distance Separable).

Dans cette thèse, on s'intéresse à un des principes fondamentaux de la cryptographie symétrique [41] (plus spécifiquement du chiffrement itératif par bloc), qui est celui de la diffusion (une permutation linéaire), tel que chaque bit du texte clair doit avoir une grande influence sur le texte chiffré. Cet intérêt se porte sur la construction des matrices MDS de diffusion à partir des codes correcteurs d'erreurs.

La première partie de cette thèse est faite afin de permettre une bonne compréhension des autres parties. Elle présente dans son premier chapitre les outils mathématiques nécessaires en théorie des codes. Tandis que le deuxième chapitre est consacré aux notions de base des codes sur les différentes structures mathématiques : alphabets finis, corps finis et anneaux.

La deuxième partie se penche sur l'étude des codes sur les anneaux. Précisément, elle contient une généralisation des travaux de K. Lally et P. Fitzpatrick sur la représentation polynomiale des codes quasi-cycliques [23] au cas des codes définis sur l'anneau $\mathcal{A} = \mathbb{F}[x]/f(x)$, où $\mathbb{F}$ est un corps fini et $f(x)$ est un polynôme unitaire quelconque. Le premier chapitre introduit des définitions et des résultat basiques de ces codes en tant que $\mathcal{A}$-modules, et examine la dualité. Le résultat principal de cette partie est la construction d'une matrice génératrice canonique et d'un système générateur du dual. Le deuxième chapitre présente la notion de l'image q-aire de ces codes, tel que q est la caractéristique du corps $\mathbb{F}$, ce qui conduit à comparer la dualité binaire à la dualité sur $\mathcal{A}$ de ces codes.

La troisième partie est une étude des codes additifs de longueur s sur le groupe commutatif $\mathcal{F} = (\mathbb{F}_2^m, +)$, les mots de ces codes sont des s-uplets de m-uplets binaires. On appelle ces codes des $\mathcal{F}$-codes ou m-bloc codes. On s'intéresse aux propriétés entre les blocs. Cette étude se limite aux codes additifs systématiques. Le premier chapitre démontre que certaines propriétés des codes sur les corps finis restent vraies pour ce type de codes, la définition d'une

image binaire de ces codes a éclairci le lien entre les codes linéaires sur $\mathbb{F}_{2^m}$ et les $\mathcal{F}$-codes, en outre une définition des codes additifs MDS est donnée. Ce chapitre se termine par une exploration des structures d'anneau possibles sur $\mathcal{F}$, afin de déterminer ceux qui seront utiles dans la construction de matrices MDS pour la cryptographie, qui est l'objet de la dernière partie de cette thèse. La définition de la matrice génératrice d'un $\mathcal{F}$-code, avec des coefficients dans l'anneau $\mathcal{L}$ des $\mathbb{F}_2$ endomorphismes de $\mathcal{F}$ dans $\mathcal{F}$, a permis l'élaboration des codes sur $\mathcal{L}$ dans le dernier chapitre de cette partie.

La quatrième partie contient les résultats principaux de cette thèse. La construction des matrices MDS pour la diffusion a fait déjà l'objet de plusieurs études. En 2011 Guo et al. dans [21] et [20] ont utilisé des matrices MDS de diffusion de taille 4×4 construites à partir du produit des matrices compagnons. En 2012 dans [37] Sajadieh et al. ont pu distinguer des matrices MDS de diffusion efficaces, en employant la construction itérative sur le produit des matrices compagnons. En 2013, Daniel Augot et Matthieu Finiasz ont présentés dans [2] de nouveaux algorithmes itératifs pour la construction de matrices MDS de diffusion, ils ont aussi remplacés la multiplication par des transformations $\mathbb{F}_2$-linéaires. Ces travaux et d'autres comme [47], dédiés à la construction de matrices MDS pour la diffusion, ont porté sur des structures commutatives. En revanche dans cette partie on étudie la construction de ces matrices à partir des codes additifs MDS sur l'anneau non commutatif $\mathcal{L}$.

Le premier chapitre introduit la notion de matrices MDS de diffusion pour la cryptographie, et présente quelques exemples de constructions sur les corps finis, en utilisant les résultats des chapitres précédents.

Le deuxième chapitre précise les différents critères des matrices MDS souhaitables pour la cryptographie symétrique, notamment la taille des blocs qui est limitée aux valeurs 4 ou 8. Pour des raisons d'implémentations machine les matrices ont été choisies avec des propriétés de symétrie, en particulier des matrices dyadiques et circulantes. Une méthodologie de recherche est donnée pour la recherche exhaustive sur ces matrices sous certaines contraintes d'optimisation pour la cryptographie.

Le troisième chapitre donne une construction de matrices dyadiques à partir de la famille des codes de Reed Solomon généralisés, cette construction est duale de celle donnée à partir des codes de Cauchy [48]. On prouve également que les codes GRS ne permettent pas de construire des matrices circulantes MDS.

Première partie

Notions préliminaires

Partie I :
Notions préliminaires

Introduction :

Le but de cette partie est de permettre une compréhension facile de cette thèse. Elle présente dans son premier chapitre un rappel des principales notions mathématiques utilisées en théorie des codes, notamment sur les anneaux et les corps finis. Tandis que le deuxième chapitre est consacré aux rappels sur différents types de codes : codes non linéaires, codes linéaires et codes additifs. Ces notions seront utilisées dans le reste de cette thèse. Pour ces énoncés, on s'est inspiré de [1] pour la partie mathématique et de [26] pour la théorie des codes.

Chapitre 1

Mathématiques pour les codes

1.1 Anneaux

La notion d'anneau est née au sein de l'école allemande du 19ème siècle, avec Kummer, Dedekind, Kronecker et Hilbert. Cependant la définition d'anneau est relativement récente et date de 1920.

Un anneau est une structure algébrique, ensemble ou domaine dans lequel on peut additionner, soustraire ou multiplier comme à l'accoutumée avec des entiers.

Nous examinons dans ce qui suit quelques définitions et propriétés des anneaux, qui seront utilisées par la suite dans l'étude des codes de cette thèse.

1.1.1 Définitions et propriétés fondamentales

Définition 1. *Un anneau A est un ensemble non vide, muni de deux lois de composition interne, souvent notés par $(+)$ et $(.)$ (par analogie aux nombres entiers) tel que :*

- *l'ensemble $(A, +)$ est un groupe commutatif.*
- *$(.)$ est distributive par rapport à $(+)$.*
- *$(.)$ est associative.*

Il s'agit d'un groupe abélien, noté additivement, sur lequel est défini une deuxième loi interne notée multiplicativement. Cette deuxième loi est associative et distributive par rapport à la première. Si, de plus, la deuxième loi est commutative alors l'anneau est dit commutatif. Et si, l'anneau A possède un élément neutre pour la deuxième loi (souvent noté 1_A), alors A est dit unitaire.

Dans la suite on considère $(A, +, .)$ un anneau unitaire, x et y deux éléments de A.

A est dit intègre, s'il ne possède pas de diviseurs de zéro, autrement dit, si $x.y = 0$ implique que x est nul ou y est nul.

Dans le cas où A n'est pas intègre, x est appelé diviseur à gauche et y est diviseur à droite. Si A est abélien les deux notions coïncident et on parlera simplement de diviseurs de zéro.

Les éléments nilpotents sont un type de diviseurs de zéro, on les définit ainsi : on considère toujours l'anneau A, et x élément de A, on dit que x est nilpotent s'il existe un entier n tel que $x^n = 0$.

En mathématique et en informatique, le concept d'idempotence signifie essentiellement qu'une opération a le même effet, qu'on l'applique une ou plusieurs fois. Un élément de x est dit idempotent si $x^2 = x$. On note que 0_A et 1_A sont des idempotents triviaux.

Soit B un anneau fini, un homomorphisme d'anneau est une application g, de A dans B, vérifiant les trois conditions suivantes, pour tout x, y dans A :

— $g(x + y) = g(x) + g(y)$.
— $g(x.y) = g(x).g(y)$.
— $g(1_A) = 1_B$.

On parle d'endomorphisme si $A = B$, d'isomorphisme si l'application g est bijective et d'automorphisme s'il y a la bijectivité et l'égalité des deux ensembles.

Soit B une partie de A, $(B, +, .)$ est un sous-anneau de A si $(B, +, .)$ est un anneau tel que 1_A est l'élément neutre de la loi "." sur B.

Une partie I de A est dite un idéal à gauche de A, si I est un sous groupe de A, et pour tout x de I et a de A, le produit $a.x$ est un élément de I. De la même manière on peut définir un idéal à droite, mais au lieu d'exiger que $a.x$ soit dans A, il faut exiger que $x.a$ soit dans A. Dans le cas commutatif les deux notions sont confondues et on parle alors d'idéal tout court. Si $1 \in I$ alors $I = A$.

Un anneau A est dit semi-simple s'il est isomorphe à un produit de corps. Soit I un idéal propre de A (différent de A), I est dit maximal si pour tout idéal J de A on a : $I \subset J$ alors $J = A$ *ou* $I = J$.

Remarque 1. *Si un idéal est un sous-anneau, alors* $1_A \in I$ *et donc* $1_A.x \in I$ *(selon la définition d'un idéal), ainsi* $A = I$.

Théorème 1. *(Krull) Tout idéal* $I \neq A$ *d'un anneau commutatif* A *est inclus dans un idéal maximal.*

Démonstration. L'ensemble des idéaux propres de A contenant I, forme une famille totalement ordonnée, et la réunion de ces idéaux est encore un idéal distinct de A, ce qui montre qu'ils possèdent un idéal maximal selon le théorème de *Zorn*. □

Définition 2. *Soit* A *un anneau abélien, et* I *un idéal de* A, I *est un idéal principal si* $I = aA$ *avec* a *dans* A.

Cette définition nous amène directement à celle d'un anneau principal.
Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.

1.1.2 Anneaux quotients

L'étude des anneaux quotients nécessite une introduction sur les relations d'équivalence.

Définition 3. *Une relation binaire R sur un ensemble E est définie par une partie E_R de $E \times E$ telle que aRb (a est en relation avec b) si et seulement si $(a, b) \in E_R$.*

Une relation binaire R sur un ensemble E est une relation d'équivalence si et seulement si R est réflexive, symétrique et transitive.

Pour tout élément x de E, on appelle classe d'équivalence de x modulo R, notée $\overline{x}$, l'ensemble $\overline{x} = \{y \in E / yRx\}$.

L'ensemble des classes d'équivalences de x modulo R est appelé l'ensemble quotient de E par R, et noté E/R.

La résolution de certaines équations simples en arithmétique sur $\mathbb{Z}$ peut s'avérer un peu plus complexe sur $\mathbb{Z}/b\mathbb{Z}$, et la primalité de b joue un rôle très décisif. Si b est un nombre premier alors $\mathbb{Z}/b\mathbb{Z}$ est un corps ce qui permet de bénéficier de la richesse de cette structure.

Définition 4. *Soient E et F deux ensembles, et f une application de E dans F. Si A est une partie de E et B est une partie de F, tel que $\forall a \in A$ on a $f(a) \in B$, alors f est l'application induite par f sur A.*

Soit I un idéal de A, on définit l'anneau quotient A/I comme l'ensemble des classes d'équivalences de la relation induite par I sur A.
D'où la proposition :

Proposition 1. *On considère l'anneau commutatif A, et I un idéal de A. L'anneau quotient A/I est un anneau pour l'addition et la multiplication induite, tel que : $\overline{a} + \overline{b} = \overline{a+b}$, et $\overline{a}.\overline{b} = \overline{a.b}$.*

Démonstration. La démonstration est assez directe, si on pose $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$. Donc $a' = a + e$ et $b' = b + t$, avec e, t dans I. Cependant $a'b' = (a.b) + (a.e + t.b + e.t)$. □

On en déduit immédiatement le théorème suivant.

Théorème 2. *On considère le morphisme d'anneaux $f : A \to B$, il existe un unique morphisme d'anneaux :*

$$\begin{array}{rccc} g & : & A/ker(f) & \to & B \\ & & g & \mapsto & g \; o \; p \end{array}$$

Où p est la surjection canonique de A dans $ker(f)$. De plus $A/Ker(f)$ est isomorphe à $Im(f)$.

Un idéal I est dit premier, si A/I est intègre.

Proposition 2. *Soit I un idéal, I est maximal si et seulement si A/I est un corps.*

Démonstration. I maximal $\Rightarrow A/I$ est un corps.
Soit $\overline{x}$ un élément de A/I, on prend l'idéal $I+xA$ qui contient I. I est maximal alors $A = I + xA$, et 1 peut s'écrire sous la présentation suivante : $1 = b + xa$ avec a dans A et b dans I. En conséquence $\overline{x}$ est inversible.
A/I est un corps $\Rightarrow I$ est maximal.
Supposons qu'il existe un idéal J de A, tel qu'il contient strictement I. On prend un élément x de J tel que $x \notin I$. Alors $\overline{x}$ est inversible dans A/I ce qui veut dire que $1 = \overline{xa}$, pour $a \in A$. D'une autre manière $1 = xa + i$, pour $i \in I$, alors i et x sont dans J. Ce qui implique que $J = A$.

□

En théorie des anneaux, le théorème des restes chinois est fondamental. Il permet entre autres d'effectuer la multiplication rapide des polynômes.

Théorème 3 (Théorème des restes chinois)**.** *Soit A un anneau commutatif, et (I, J) deux idéaux de A, tels que $I + J = A$ (avec $I + J = (x + y)$ pour x de I et y de J).*
Pour a, b de A, il existe un élément e dans A, tel que :
$e = a \ mod \ I$ et $e = b \ mod \ J$.

Démonstration. Si on considère le fait que $1 \in A$, et que $I + J = A$, alors il existe deux éléments x et y de I et J respectivement, tels que : $1_A = x + y$. On considère e un élément de A, alors $e = x.\alpha + y.\beta$, ainsi $e - y.\beta = x.\alpha$ est un élément, par la suite $e = y\beta \ mod \ I$. En revanche, on sait que $y = 1 - x = 1 \ mod \ I$, alors $e = \beta \ mod \ I$. De la même manière, on peut montrer que $e = \alpha \ mod \ J$.

□

1.1.3 Anneaux de polynômes

Soit E un ensemble, et x une indéterminée de E (notée S la première fois par Diophante en 3 ème siècle afin de résoudre les équations dites diophantiennes). La structure donnée par les puissances du polynôme x multipliées par les éléments de E est notée $E[x]$.

On note que E ne doit pas forcément vérifier beaucoup de contraintes, il faut juste qu'il supporte l'addition et la multiplication.

Si E est un anneau commutatif alors $E[x]$ est l'anneau de polynômes à coefficients dans E, et possède les caractéristiques d'un anneau commutatif.

Dans ce qui suit on considère l'anneau des polynômes $A[x]$ où A est un anneau quelconque.

D'après la définition d'un anneau de polynôme donnée ci-dessus, un polynôme P de $A[x]$, est de la forme :

$$P(x) = a_0.x^0 + a_1.x^1 + \ldots + a_n.x^n, \text{ pour } a_i \text{ dans } A, \text{ et } 0 \leq i \leq n.$$

Deux polynômes sont égaux si et seulement si leurs coefficients du même rang sont égaux.

Si on pose plus de structure sur A, spécifiquement si chaque élément est inversible pour la deuxième loi, alors la structure $A[x]$ possédera la division euclidienne. Ainsi il devient possible d'utiliser les éléments de l'arithmétique, voir l'identité de Bézout, ou le théorème fondamental de l'arithmétique.

Lemme 1. *Soit $A[x]$ l'anneau de polynômes à coefficients dans A, les propriétés suivantes sont équivalentes :*

1. *A est intègre.*
2. *$A[x]$ est intègre.*
3. *Si f, g sont deux polynômes non nuls de $A[x]$, $deg(f.g) = deg(f)+deg(g)$.*

Démonstration. On commence par montrer que (1) $\Rightarrow$ (3).
Soient f, g deux polynômes non nuls de $A[x]$ (si un des f ou g est nul l'égalité est triviale). $f(x) = \sum_{i=0}^{i=m} a_i x^i$ et $g(x) = \sum_{j=0}^{j=n} b_j x^j$ avec $a_i, b_j \in A$ et a_n, b_m sont non nuls.
$f(x).g(x) = \sum_{t=0}^{t=n+m} a_t.b_t\, x^t$, et puisque A est intègre, alors $deg(f.g) = deg(f)+deg(g)$.
(3) $\Rightarrow$ (2).
Soient f, g deux polynômes non nuls de $A[x]$ tels que $f(x).g(x) = 0$, on sait que $deg(f.g) = deg(f)+deg(g)$, alors $deg(f)+deg(g) = 0$ ce qui est impossible vu que le degré est toujours positif.
(2) $\Rightarrow$ (1).
On voit immédiatement qu'un sous-anneau d'un anneau intègre est intègre. □

On note que $deg(c) = 0$ pour c constante non nul, et $deg(0) = -\infty$.

1.2 Modules

Suite à l'étude de l'anneau dans ses différentes formes de la section précédente, une autre manière utile d'étude de cette structure est d'examiner son action sur un groupe abélien. Une telle action s'appelle un module sur un anneau (par défaut commutatif et unitaire). La notion de module peut être vue comme une généralisation de celle d'espace vectoriel. Cette généralisation n'est pas inutile, puisqu'elle apparaît dans beaucoup de contextes algébriques et géométriques, et spécifiquement elle sera la principale structure de la partie II de cette thèse.

Définition et propriétés fondamentales

Désormais on supposera que tous les anneaux sont commutatifs et unitaires.

Définition 5. *Soient $(M, +)$ un groupe commutatif et A un anneau unitaire. On suppose de plus que M est muni d'une loi externe, de $A \times M$ sur M, qu'on note "."*.

$(M, +, .)$ est un A-module à gauche si, pour tous a, b de A et x, y de M on a :

— $a.(x+y) = a.x + a.y$
— $(a+b).x = a.x + b.x$
— $(ab)x = a(bx)$
— $1.x = x$

On peut définir de la même manière un A-module à droite, en plaçant les éléments de A à droite.

Soit M un A-module a gauche, et N un sous-groupe de $(M, +)$, on dit que N est un sous-module (à gauche) si pour tout $a \in M$ et $x \in N$, $a.x$ est dans N.

Autrement dit, un sous-module est une partie linéairement stable.

Si le module est un espace vectoriel on parle de sous-espace vectoriel.

Un module sur un anneau A est dit simple s'il est différent du module nul, et s'il n'existe pas de sous module de M en dehors de $\{0\}$ et M. Soit M un module, M est dit :

— de type fini, si son système de générateur est de cardinal fini.
— noethérien, si tous ses sous-modules sont de type fini.
— artinien, si toute suite décroissante de sous-modules de M est stationnaire. Cela est équivalent à dire que toute partie non vide de sous-modules de M admet un élément minimal.

Un module est dit semi-simple, s'il est somme directe de sous-modules simple, autrement dit, s'il est complètement réductible.

Proposition 3. *Un module simple est indécomposable, c-à-d qu'il n'est pas isomorphe à une somme directe de deux modules non nuls. La réciproque est fausse.*

Produit de Hadamard

Définition 6.

Soient $M = (a_{i,j})$ et $N = (b_{i,j})$ deux matrices de même dimension, on appelle produit de Hadamard de M et N le produit terme à terme, tout comme l'addition. On le note avec le signe $\star$ tel que : $M \star N = (a_{i,j}.b_{i,j})$.

Exemple 1. *Soient* $M = \begin{pmatrix} 3 & 2 & -1 \\ 0 & 2 & 0 \end{pmatrix}$ *et* $N = \begin{pmatrix} 1 & 3 & 4 \\ 6 & 1 & -1 \end{pmatrix}$, *le produit de Hadamard de M et N est* $M \star N = \begin{pmatrix} 3 & 6 & -4 \\ 0 & 2 & 0 \end{pmatrix}$

1.3 Espaces vectoriels et corps finis

L'étude des corps finis, également appelés corps de Galois, est indispensable en théorie des codes correcteurs d'erreurs.

On rappelle qu'un corps est un anneau dans lequel les éléments non nuls ont un inverse pour la multiplication (autrement dit : l'ensemble des éléments non nuls est un groupe pour la multiplication).

Un corps fini, comme son nom l'indique, est un corps qui contient un nombre fini d'éléments. C'est un corps commutatif (d'après le théorème de Wedderburn), entièrement déterminé par son cardinal. Ce dernier est toujours une puissance d'un nombre premier.

Le théorème suivant permet de caractériser l'inversibilité dans certains cas :

Théorème 4.
- *Soit k un entier de $\mathbb{Z}$, k est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $pgcd(k, n) = 1$.*
- *Soit $q(x)$ un polynôme de $K[x]$, $q(x)$ est inversible dans l'anneau $K[x]/(p(x))$ si et seulement si $pgcd(p(x), q(x)) = 1$.*

On rappelle qu'un polynôme $p(x)$ à coefficients dans le corps K admet a comme racine dans K, si et seulement s'il est divisible par le polynômes $(x - a)$. En particulier, un polynôme irréductible de degré supérieur à 2 n'a pas de racine dans K. La réciproque est fausse.

Notons que la décomposition en facteurs irréductibles dans les anneaux $\mathbb{Z}$ et $K[x]$, est unique. En particulier :

Proposition 4. *Soit $K[x]$ un anneau, et $p(x)$ un polynôme à coefficients sur K. Le nombre de racines de $p(x)$ est inférieur ou égal à son degré.*

La proposition suivante est une conséquence du théorème 4 :

Proposition 5. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier. De même l'anneau $K[x]/(p(x))$ est un corps si est seulement si le polynôme $p(x)$ est irréductible.*

1.3.1 Espaces vectoriels

Dans ce qui suit, on considère K un corps commutatif.

Un espace vectoriel est un ensemble muni de structure permettant de faire des combinaisons linéaires. Plus précisément, soit E un ensemble muni de deux lois, dont la première est une loi de composition interne notée additivement $(+)$, et la deuxième est une loi de composition externe de $K \times E$ dans E, notée multiplicativement $(.)$.

On note 1 l'élément neutre pour la multiplication de K, et 0 l'élément neutre pour l'addition de K.

On dit que E est un espace vectoriel sur le corps K, si les deux conditions suivantes sont vérifiées :

1. $(E, +)$ est un groupe abélien.
2. $\forall (x, y) \in E^2$, $\forall (\lambda, \mu) \in K^2$:
   - $\lambda.(x + y) = \lambda.x + \lambda.y$.
   - $(\lambda + \mu).x = \lambda.x + \mu.x$.
   - $\lambda.(\mu.x) = (\lambda\mu).x$.
   - $1.x = x$

Soit E_1, une partie non vide d'un espace vectoriel E. E_1 est dit un sous-espace vectoriel de E, s'il est stable par combinaison linéaire.

Puisque l'addition est la muticplication scalaire sont définis aussi sur E_1, alors on peut déduire qu'un sous-espace vectoriel d'un espace vectoriel est un espace vectoriel.

Les élḿents d'un espace vectoriel sont appelés vecteurs.

L'intersection de sous-espaces vectoriels d'un espace vectoriel E est un sous-espace vectoriel de E.

Une application de deux espaces vectoriels sur un même corps K, ou de deux modules sur un même anneau A, qui préserve l'addition des vecteurs et la multiplication scalaire est appelée une application linéaire ou un morphisme.

Définition 7. *Soient E et F deux espaces vectoriels sur un corps K, et f une application de E dans F. f est une application linéaire, si elle préserve les opérations définis sur E, autrement dit, si :*

$$\forall (x, y) \in E^2, (\lambda, \beta) \in K^2, f(\lambda x + \beta y) = \lambda f(x) + \beta f(y).$$

L'ensemble des applications linéaires de E dans F est un espace vectoriel sur le corps K.

Soient E_1 et E_2 deux espaces vectoriels de E, la somme de E_1 et E_2, est le sous-espace vectoriel engendré par $E_1 \cup E_2$. On le note par $E_1 + E_2$.

Proposition 6. *Soient E_1 et E_2 deux sous-espaces vectoriel, la somme de E_1 et E_2 est : $E_1 + E_2 = \{x_1 + x_2 / x_1 \in E_1$ et $x_2 \in E_2\}$.*

Définition 8. *On considère E_1 et E_2, deux sous-espaces vectoriels. On dit que E est somme directe de E_1 et E_2, et on note : $E = E_1 \oplus E_2$, si les deux conditions suivantes sont vérifiées :*

1. $E = E_1 + E_2$.
2. $E_1 \cap E_2 = \{0\}$.

Proposition 7. *Un espace vectoriel E est la somme directe de deux sous-espaces vectoriels E_1 et E_2, si et seulement si :*

$$\forall x \in E,\ \exists!(x_1, x_2) \in E_1 \times E_2,\ x = x_1 + x_2.$$

Démonstration. On démontre cette équivalence dans les deux sens :

— $E = E_1 \oplus E_2 \Rightarrow \forall x \in E, \exists!(x_1, x_2) \in E_1 \times E_2, x = x_1 + x_2$.
On commence par montrer l'existence, puis on montre l'unicité.
Soit x un élément de E, on suppose que E est la somme directe de E_1 et E_2. Alors $E = E_1 + E_2$, ainsi $\exists x_1 \in E_1$ et $\exists x_2 \in E_2$, tels que $x = x_1 + x_2$. Pour montrer l'unicité on suppose que : $\exists x'_1 \in E_1$ et $\exists x'_2 \in E_2$, tels que $x = x'_1 + x'_2$. Donc $x_1 - x'_1 = x'_2 - x_2$. Or on sait que $x_1 - x'_1 \in E_1$ et $x'_2 - x_2 \in E_2$. En revanche, d'après la définition 8, $E_1 \cap E_2 = \{0\}$. Par conséquence $x_1 - x'_1 = 0$ et $x'_2 - x_2 = 0$. D'où l'unicité.

— $\forall x \in E, \exists!(x_1, x_2) \in E_1 \times E_2, x = x_1 + x_2 \Rightarrow E = E_1 \oplus E_2$.
Soit x un élément de E, on suppose que pour tout $x \in E$, $x = x_1 + x_2$ tels que $x_1 \in E_1$ et $x_2 \in E_2$. Il est clair que E est somme de E_1 et E_2, on montre que cette somme est directe :
On suppose $\exists x \in E_1 \cup E_2$, x peut être écrit comme $x = x + 0$ avec $x \in E_1$ et $0 \in E_2$. On peut écrire aussi x sous la forme : $x = 0 + x$ avec $0 \in E_1$ et $x \in E_2$. Et puisque l'unicité de l'existence des élément de la décomposition impose que $x = 0$. Alors $E = E_1 \oplus E_2$.

□

Le théorème suivant est une généralisation de la proposition précédente :

Théorème 5. *Soit $n \in \mathbb{N}^*$ et soient $E_1, E_2, \dots E_n$, n sous-espaces vectoriels d'un espace vectoriel E. Les conditions suivantes sont équivalentes :*

1. *Tout élément de E, s'écrit de manière unique $x = x_1 + x_2 + \cdots + x_n$, avec, pour tout $i \in \{1, \dots, n\}, x_i \in E_i$.*
2. *$E = E_1 + E_2 + cldots + E_n$, et pour tout $i \in \{1, \dots, n\}$. $E_i \cap (\sum_{j \neq i} E_j) = \{0\}$.*

Si l'une de ces conditions est vérifiée, on dit que E est la somme directe des E_i, et on écrit : $E = E_1 \oplus E_2 \oplus \dots \oplus E_n = \oplus_{i=1}^{n} E_i$.

Démonstration. La démonstration de ce théorème est une généralisation de celle de la proposition précédente. Montrons l'équivalence des deux conditions :
1) $\Rightarrow$ 2) : On suppose que $x \neq 0$ et que $x \in E_i \cup (\sum_{j \neq i} E_j)$, pour $i \in \{1, \dots, n\}$. L'élément x se décompose alors en $x = x + 0$ avec $x \in E_i$ et $0 \in (\sum_{j \neq i} E_j)$, et en $x = 0 + x$, avec $0 \in E_i$ et $x \in (\sum_{j \neq i} E_j)$, et puisque on a l'unicité de la décomposition alors $x = 0$, ce qui contredit l'hypothèse $x \neq 0$. On a donc bien $x = 0$.
2) $\Rightarrow$ 1) : Soit x un élément de E, on suppose que x a deux décompositions différentes : $x = x_1 + x_2 + \dots + x_n = x'_1 + x'_2 + \dots + x'_n$. Alors $x_1 - x'_1 = (x'_2 - x_2) + (x'_3 - x_3) + \dots + (x'_n - x_n)$. Et vu que $E_i \cap (\sum_{j \neq i} E_j) = \{0\}$, alors $x_1 = x'_1$ et $(x'_2 - x_2) + (x'_3 - x_3) + \dots + (x'_n - x_n) = 0$, et ainsi on montre par récurrence que $x_i = x'_i$ pour $i \in \{2, \dots, n\}$.

□

1.3.2 Corps finis

L'arithmétique modulaire à partir de l'anneau $\mathbb{Z}$, permet de construire un type particulier de corps finis qui est celui des anneaux $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Il contient exactement les éléments suivants $\{0, 1, \dots, p-1\}$. Cette classe de corps intervient dans la construction de tous les corps finis. Le nombre p est toujours un nombre premier, de plus c'est la caractéristique du corps.

$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ est un exemple particulier très important de corps fini à 2 éléments.

On note que si K et L sont deux corps finis, tels que $K \subset L$, on peut doter L de la structure d'un K-espace vectoriel. Ainsi on peut avoir une relation entre le cardinal de L et le cardinal de K : $|L| = |K|^{dim_K(L)}$.

Définition 9. *Soit K un corps fini, le sous corps premier de K est le plus petit sous-corps de K contenant* 1.

Le théorème suivant appelé théorème de l'élément primitif, est un résultat principal dans l'étude des corps fini :

Théorème 6. *Soit K, un corps fini, le groupe multiplicatif K^* de K, est un groupe cyclique. Tout générateur de ce groupe est appelé élément primitif de K.*

Soit p la caractéristique du corps fini K et α un élément primitif de K. $K = \mathbb{F}_p(\alpha)$, d'après le théorème 6 on a la proposition suivante :

Proposition 8. *Tout corps fini de caractéristique p est une extension algébrique simple de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Soit q le cardinal du corps K. On sait que tout élément du groupe multiplicatif K^* de K a pour ordre un diviseur de $q-1$, alors on en déduit que tout élément de K est une racine de $x^q - x$. D'où la proposition suivante :

Proposition 9. *Soit K un corps fini à q éléments. On a la factorisation suivante :*

$$x^q - x = \prod_{\alpha \in K}(x - \alpha)$$

Chapitre 2

Autour des codes correcteurs d'erreurs

2.1 Le codage

La transmission et le stockage des données ne sont pas à l'abri des bruits qui peuvent les affecter à travers les canaux de communication non fiables.

Supposons qu'on désire envoyer une information à travers un canal de transmission, l'information reçue à la réception peut contenir des éventuelles erreurs dues au bruit. Si on se place dans le cas d'un codage binaire, le message à envoyer sera une suite de bits $\{0, 1\}$.

Le principe des codes correcteurs d'erreurs consiste à ajouter de la redondance à l'information qu'on désire envoyer. Qui dit ajouter de la redondance avant d'envoyer (le codage) dit aussi l'enlever à la réception (le décodage) dans le but de récupérer l'information intègre. Malheureusement la théorie des codes n'assure pas toujours l'intégrité de l'information à cent pour cent. Cela dépend de la qualité du canal de transmission, ainsi que de la capacité de détection et/ou de correction du code utilisé, c'est-à-dire le nombre des erreurs que ce code peut détecter et/ou corriger.

Application d'encodage

Soient k et n des nombres entiers naturels, E un ensemble non vide, et f une application injective de E^k dans E^n. Soit $a = (a_1, a_2, \ldots, a_k)$ un élément de E^k, et c sont image par f tel que :

$$f(a) = c = (c_1, c_2, \ldots, c_n), \text{ tel que } k \leq n.$$

Cette construction de certains éléments c de E^n à partir des éléments a de E^k est une application d'encodage. Le sous-ensemble $C = f(E^k)$ des éléments de E^n ayant des antécédents dans E^k par f, est appelé code associé à l'application d'encodage f. On note que f est bijective entre E^k et C.

2.2 Codes sur un alphabet fini

Rappelons d'abord qu'un alphabet est un ensemble fini non vide d'éléments appelés lettres ou symboles.

Définition 10. *Soit E un alphabet fini de taille q. Un code C de longueur n sur E est une partie de E^n, c'est-à-dire un ensemble d'éléments $c = (c_1, c_2, \ldots, c_n)$ de même longueur n appelés mots, avec $c_i \in E$ pour tout $0 \leq i \leq n$.*

2.2.1 Distance de Hamming

On note que le cardinal de C est le nombre de ces mots. La distance de Hamming, est une propriété combinatoire non algébrique (c'est bien là la difficulté de la théorie des codes) de base de la théorie des codes correcteurs d'erreurs, et qui doit son nom à Richard Hamming [22]. C'est une quantité mathématique, qui quantifie le nombre de coordonnées distinctes entre deux séquences de lettres.

Définition 11. *Soient $a = (a_1, a_2, \ldots, a_n)$ et $b = (b_1, b_2, \ldots, b_n)$ deux mots de longueur n sur E, la distance de Hamming, notée $d_H(a, b)$, entre les deux mots a et b est :*

$$d_H(a, b) = |\{i \mid a_i \neq b_i \text{ pour } 1 \leq i \leq n\}|.$$

De plus :

$$d_H(a, b) = d_H(a_1, b_1) + d_H(a_2, b_2) + \ldots + d_H(a_n, b_n)$$

tels que, si a_i et b_i sont deux mots de longueur 1 de E, et :

$$d_H(a_i, b_i) = \begin{cases} 1 & si \quad a_i \neq b_i. \\ 0 & si \quad a_i = b_i. \end{cases}$$

Étant donné que d_H est une distance, la proposition suivante cite les principales propriétés de cette distance :

Proposition 10. *La distance de Hamming d_H est une distance, en particulier, si a, b, c sont des mots de longueur n sur E, alors :*

1. $0 \leq d_H(a, b) \leq n$.
2. $d_H(a, b) = 0$ *si et seulement si* $a = b$.
3. $d_H(a, b) = d_H(b, a)$.
4. $d_H(a, c) \leq d_H(a, b) + d_H(b, c)$.

Démonstration. Les trois premières propriétés sont évidentes à partir de la définition 11.

Procédons par récurrence sur n pour démontrer la dernière :
Pour $n = 1$, il est évident que $d_H(a, c) \leq d_H(a, b) + d_H(b, c)$. Supposons que la

propriété est vraie pour n, et démontrons la pour $n+1$:
Supposons que :

$$d_H((a_1,\ldots,a_n),(c_1,\ldots,c_n))$$
$$\leq$$
$$d_H((a_1,\ldots,a_n),(b_1,\ldots,b_n)) + d_H((b_1,\ldots,b_n),(c_1,\ldots,c_n))$$

Et puisque :

$$d_H(a_{n+1},c_{n+1}) \leq d_H(a_{n+1},b_{n+1}) + d_H(b_{n+1},c_{n+1})$$

Alors :

$$d_H((a_1,\ldots,a_n),(c_1,\ldots,c_n)) + d_H(a_{n+1},c_{n+1})$$
$$\leq$$
$$d_H((a_1,\ldots,a_n),(b_1,\ldots,b_n))$$
$$+$$
$$d_H((b_1,\ldots,b_n),(c_1,\ldots,c_n))$$
$$+$$
$$d_H(a_{n+1},b_{n+1}) + d_H(b_{n+1},c_{n+1}).$$

On déduit de ces relations que :

$$d_H(a,c) \leq d_H(a,b) + d_H(b,c)$$

pour tout n. □

2.2.2 Distance minimale

La distance minimale d d'un code C, est le minimum des distances de Hamming entre ses mots distincts (on suppose que C a au moins deux mots).

Le poids de Hamming $w(c)$ (ou juste poids) d'un mot c, est le nombre des coordonnées non nulles de c.

Exemple 2. *En partant du cas où l'alphabet E est $E = \mathbb{F}_2 = \{0,1\}$. Un code sur $\mathbb{F}_2$ est appelé code binaire.*

Soit C le code binaire : $C = \{(0,1,1);(0,1,0);(1,1,1)\}$.
C est de longueur $n = 3$, de cardinal $|C| = 3$, et de distance minimale $d = 1$.
La distance de Hamming entre les deux mots $(0,1,1)$ et $(0,1,0)$ de C, est $d((0,1,1);(0,1,0)) = 1$.

La technique de codage repose sur la redondance dans le but de pouvoir détecter et/ou corriger les erreurs de transmission. Notamment on ajoute à chaque mot de k lettres une séquence de r éléments appelée la redondance.

Un code de longueur n, de distance minimale d et de dimension k est appelé un (n,k,d)-code, ou code de paramètres (n,k,d) (La notation $[n,k,d]$ est réservée aux codes linéaires).

On précise que, par abus de langage, on parle ici de dimension k dans le cas général (linéaire et non linéaire), telle qu'elle quantifie la longueur du mot avant le codage (avant l'ajout de la redondance $r = n - k$).

On appelle capacité de détection $e = d-1$ d'un code C, le nombre maximal d'erreurs que le code est capable de détecter. La capacité de correction $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ est le nombre maximal d'erreurs que le code permet de corriger sans ambiguïté.

Proposition 11. *Soit C un code de distance minimale d, les boules fermées de rayon r centrées sur les mots du code, sont disjointes si $r \leq t$ avec $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.*

Démonstration. On suppose qu'il y a au moins deux boules de centres c_1 et c_2 respectivement, et y un mot de leur intersection. Alors $d(c_1, c_2) = d(c_1, y) + d(y, c_2) \leq 2t$, et puisque $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, alors

$$d(c_1, c_2) \leq 2t \leq 2\frac{d-1}{2} \leq d - 1 \leq d$$

ce qui est absurde. □

2.2.3 Borne de Singleton

Dans [44], Richard C. Singleton démontre l'existence d'une borne, pour tout code C de paramètres $[n, k, d]$ sur un alphabet E de taille q.

Proposition 12. *Soit C un code de longueur n et de distance minimale d, sur un alphabet E de cardinal q. L'inégalité de la borne de Singleton est :*

$$|C| \leq q^{n-d+1}.$$

Démonstration. On pose $k = log_q(\#C)$ et $t = \lceil q \rceil - 1$, on remarque que $k - 1 \leq t < k$. Le nombre de t-uplets distincts d'éléments de E^t est q^t, il est strictement inférieur au nombre q^k de mots de codes distincts. Si on observe les mots de C tronqués aux t premières positions, il y a au moins deux mots $c^{(i)}$ et $c^{(j)}$ qui sont identiques sur ces t coordonnées. Ainsi $d_H(c^{(i)}, c^{(j)}) \leq n - t$. La propriété $k - 1 \leq t$ permet d'en déduire que : $d \leq d_H(c^{(i)}, c^{(j)}) \leq n - k + 1$. □

2.2.4 Codes MDS

La classe des codes à distance séparable maximale(MDS en abréviation) a été introduite pour la première fois par Richard C. Singleton dans [44].

Définition 12. *Soit C un code de cardinal q^k, de longueur $n = k + r$, et de distance minimale d. Le code C est dit MDS s'il atteint la borne de Singleton : $|C| = q^{n-d+1}$.*

Comme leur nom le laisse entendre, ce sont des codes qui ont une distance de Hamming maximale.

La construction de ce type de code n'est pas facile, d'où le recours à différentes méthodes et structures algébriques. La construction de ces codes sur une nouvelle structure algébrique sera étudiée en détails dans la Section 5.4.

2.3 Codes linéaires sur un corps fini

Soit K un corps fini. On considère les codes sur K de longueur n et d'une manière naturelle les applications d'encodages linéaires.

Définition 13. *Un code linéaire C de longueur n et de dimension k sur un corps fini $K = \mathbb{F}_q$ est un sous-espace vectoriel de K^n.*

Si la dimension de C est k, C est isomorphe à K^k, et tout isomorphisme $f : K^k \mapsto C$ est une application d'encodage linéaire.

Dans le cas d'un code linéaire, la distance de Hamming peut s'exprimer en terme de poids minimal des mots de codes :

Soient $c^{(i)}$ et $c^{(j)}$ deux mots de C, puisque C est linéaire, alors $c^{(t)} = c^{(i)} - c^{(j)}$ est un mot du code C, et par la suite : $d(c^{(i)}, c^{(j)}) = w(c^{(i)} - c^{(j)}) = w(c^{(t)})$.

La distance minimale d'un code linéaire est égale à son poids minimal $min_{c \in C, c \neq 0}(w(c))$.

2.3.1 Matrice génératrice

Puisqu'il existe une application linéaire d'encodage, celle-ci peut s'écrire sous une forme matricielle (la matrice de l'application linéaire dans la base canonique). On peut définir plus généralement une matrice génératrice d'un code ainsi :

Définition 14. *Toute matrice dont les lignes forment une base de C est une matrice génératrice d'un code C.*

Soit x un mot de K^k à encoder avec une application linéaire f, et c ($c \in K^n$) son image par f. Il existe une matrice G de taille $k \times n$ dans K telle que : $x.G = f(x) = c$. Ceci nous amène à la définition suivante :

Définition 15. *Soit C un code linéaire de longueur n et de dimension k sur un corps K. Soit G une matrice génératrice de taille $k \times n$ sur K alors :*

$$C = \{c = x.G \mid x \in K^k\}$$

Autrement dit, un code linéaire est complètement décrit par une de ses matrices génératrices.

La notion d'encodage systématique est essentielle dans la suite de notre thèse.

Définition 16. *Une matrice génératrice G est dite systématique si elle est de la forme $G = (I_k \,|\, B)$, où I_k est la matrice identité de taille k et B une matrice $k \times (n-k)$, appelée matrice de redondance du code C.*

2.3.2 Code dual

Produit scalaire

C'est une opération qui s'applique à deux vecteurs afin de leur associer un scalaire. Dans l'histoire, ce produit a été un élément important de calcul en géométrie euclidienne.

Définition 17. *Soient x et y deux éléments de l'espace vectoriel $V = K^n$ sur le corps fini K. Le produit scalaire de x et y est le scalaire :*

$$< x, y >= \sum_{i=1}^{n} x_i.y_i \in K.$$

Soit C un code linéaire de longueur n et de dimension k sur un corps fini K. La propriété de linéarité du code C vu comme étant un sous-espace vectoriel, donne naissance à la notion de son dual. Celle-ci joue un rôle important dans le décodage des messages.

Le code dual d'un code linéaire C est le sous-espace orthogonal de C, noté $C^{\perp}$:

$$C^{\perp} = \{y \in K^n \mid \ < y, c >= 0, \ \forall c \in C\}.$$

Matrice de contrôle

Étant donné que $C^{\perp}$ est un sous-espace vectoriel, sa matrice génératrice souvent notée H sera alors constituée des $(n-k)$ éléments de la base du sous-espace vectoriel sur K. Cette matrice de taille $(n-k) \times n$ est une matrice génératrice de $C^{\perp}$, et aussi appelée matrice de contrôle de C.

Propriété 1. *Soit C un code linéaire de longueur n et de dimension k sur K, et H une matrice génératrice de son code dual $C^{\perp}$. Le code C peut être aussi défini par :*

$$C = \{y \in K^n \mid y.H^t = 0\}$$

2.3.3 Codes MDS linéaires

Dans cette partie on explore quelques propriétés sur les codes MDS pour lesquelles la linéarité est indispensable. Alors dans ce qui suit on considère C un code MDS linéaire de paramètres $[n, k, d]$.

Principales propriétés des codes MDS

Nous rappelons ici sans démonstrations quelques résultats classiques sur les codes linéaires MDS. Pour plus de précisions et pour les démonstrations, on renvoie à [[26], chap 11].

Théorème 7. *Soit C un code linéaire de matrice génératrice G et de matrice de contrôle H. Le code C est MDS si et seulement si pour tout choix de $n-k$ colonnes de H, celles-ci sont linéairement indépendantes.*

Théorème 8. *Si C est un code MDS, alors son code dual $C^{\perp}$ est aussi un code MDS.*

Théorème 9. *Un code linéaire C est un code MDS si et seulement s'il possède une matrice génératrice $G = (I_k \,|\, M)$, telle que toutes les sous matrices carrées de sa matrice de redondance M sont inversibles.*

Conjecture des codes MDS

Soit C, un code linéaire MDS de dimension k sur un alphabet E de taille q. La longueur maximale (n_{max}) que peut atteindre le code C est donnée par les bornes de *Bush* [15] et de *Segre* [38], en fonction de q et k tels que :

- Si $k \geq q + 1$: $n_{max} = k + 1$.(*Bush* [1952])
- Sinon : (*Segre* [1955])
  - Si $(q = 2^h, k = 3)$ ou $(q = 2^h, k = q - 1)$: $n_{max} = q + 2$.
  - Sinon : $n_{max} = q + 1$.

2.3.4 Matrices MDS sur un corps fini

À partir d'un code C MDS de paramètres $[n, k, d]$, on peut définir la notion de matrice MDS. Cette notion sera particulièrement importante dans le cadre de son application aux matrices de diffusion en cryptographie symétrique.

Définition 18. *Soit M une matrice $k \times (n-k)$ à coefficients dans K, M est dite matrice MDS si le code K-linéaire C généré par la matrice $G = (I_k|M)$ est un code MDS.*

Par conséquent, et d'après le théorème 9, une matrice est MDS si et seulement si toutes ses sous-matrices carrées sont inversibles.

Proposition 13. *Soit M une matrice MDS de taille $k \times (n-k)$ sur le corps fini K, les propriétés suivantes sont équivalentes :*

1. *M est MDS.*
2. *M^t est MDS.*

Si de plus M est une matrice carrée, alors la propriété M^{-1} est MDS est équivalente aux deux propriétés précédentes.

Démonstration. $1 \Leftrightarrow 2$ Soit C le code MDS généré par la matrice systématique $(I_k|M)$, alors le code dual de C est généré par la matrice $(-M^T|I_k)$. $C^{\perp}$ est MDS, parce que C est MDS. Donc M^T est une matrice MDS.

$1 \Leftrightarrow 3$ Soit M une matrice MDS carrée de taille k sur K, et soit $(I_k|M)$ une matrice génératrice d'un code C. M est une matrice inversible alors on peut multiplier $(I_k|M)$ par M^{-1} ce qui donne $(M^{-1}|I_k)$. Si on permute les deux parties, on obtient la matrice $(I_k|M^{-1})$ qui est aussi une matrice génératrice d'un code MDS. □

2.3.5 Équivalence entre les matrices MDS carrées

Soit M une matrice carrée de taille k sur le corps fini $K = \mathbb{F}_{2^m}$, on définit C comme étant le code systématique linéaire de longueur r et de matrice génératrice $(I_k|M)$ avec $n = 2k$.

On pose $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in (K^*)^n$ et on définit le K-isomorphisme $\Psi_\lambda(x) = (\lambda_1 x_1, \ldots, \lambda_r x_n)$, pour $x = (x_1, \ldots, x_n) \in (K^*)^n$. Il est clair que l'application Ψ_λ préserve la distance de Hamming, alors le code C est MDS si et seulement si le code $C' = \Psi_\lambda(C)$ est MDS.

À partir de λ on construit deux matrices carrées diagonales de taille k sur K :

$$D_{\lambda,1} = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \lambda_k \end{pmatrix}$$

et

$$D_{\lambda,2} = \begin{pmatrix} \lambda_{k+1} & 0 & \ldots & 0 \\ 0 & \lambda_{k+2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \lambda_n \end{pmatrix}$$

On remarque directement que la matrice $(D_{\lambda,1} I_k | M D_{\lambda,2})$ est une matrice génératrice du code C', et que $(I_k | D_{\lambda,1}^{-1} A D_{\lambda,2})$ est sa matrice génératrice systématique.

On conclut que la matrice carrée M sur K est une matrice MDS si et seulement si la matrice $(D_{\lambda,1}^{-1} M D_{\lambda,2})$ est MDS pour λ dans $(K^*)^r$.

Une permutation de lignes ou de colonnes d'une matrice M ne changera pas l'ensemble de ses sous-déterminants. Il est aussi clair que la permutation des coordonnées des mots d'un code C ne change pas son poids de Hamming. De ce fait, une matrice M sur K est MDS si et seulement si la matrice PMP' est une matrice MDS, où P et P' sont deux matrices de permutation à coefficients dans le corps fini K.

2.4 Codes linéaires sur un module

Un code C de longueur n sur un anneau A est un sous module de E. Autrement dit, il est stable par addition et multiplication par scalaires.

On ne peut pas parler de base, puisque l'on n'a pas une structure d'espace vectoriel. Cependant si l'anneau est fini on a la notion de système générateur.

Définition 19. *Soit M un A-module, on dit que $S = (u_1, u_2, \ldots, u_n)$ est un système générateur d'un module M, si tout élément de M peut s'écrire comme une combinaison linéaire des u_i, pour $i \in \{1, \ldots, n\}$.*

Matrice génératrice

Soit C un code linéaire de longueur n sur un anneau A. Une matrice G de taille $k \times n$ est dite matrice génératrice de C, si l'application linéaire Φ de A^k dans A^n, telle que pour x de A^k : $\Phi(x) = x.G$, vérifie $\Phi(A^k) = C$.

A priori, Φ n'est pas un isomorphisme de A^k dans C, mais les lignes de G forment un système de générateurs de C. Une étude plus détaillée sur ce type de codes se fera dans la partie . Il est en particulier intéressant de construire des matrices génératrices telles que Φ soit un isomorphisme.

Deuxième partie

Codes sur un quotient d'anneau de polynômes

Partie II : Codes sur un quotient d'anneau de polynômes

Introduction :

L'objectif de cette partie est d'étudier les codes dont l'alphabet $\mathcal{A}$ est un quotient fini d'un anneau de polynômes de la forme $\mathcal{A} = \mathbb{F}[x]/f(x)$. Le cas particulier $f(x) = x^m - 1$ est bien connu et correspond à une représentation des codes quasi-cycliques définis sur $\mathbb{F}$. Notre but est de faire une étude des codes sur une structure plus générale de $\mathcal{A}$, en prenant pour $f(x)$ un polynôme unitaire quelconque.

Nous appelons les codes définis sur l'alphabet $\mathcal{A}$ des $\mathcal{A}$-codes. Notre travail généralise les travaux de K. Lally et P. Fitzpatrick sur la représentation polynomiale des codes quasi-cycliques [23]. Contrairement à leur approche, nous n'utilisons pas les bases de Gröbner, mais uniquement la division euclidienne des polynômes. Nous introduisons en particulier une matrice génératrice canonique sous la forme d'Hermite. Nous nous intéressons naturellement à l'image q-aire de ces codes, où q est le cardinal du corps fini $\mathbb{F}$. Nous étudions la dualité définie dans $\mathcal{A}^r$, et nous la comparons avec la dualité obtenue à partir de l'image q-aire. Un des résultats intéressants est que, contrairement à ce que l'on obtient dans le cas des codes quasi-cycliques ou des codes définis sur une extension de $\mathbb{F}$ (c'est-à-dire lorsque $f(x)$ est irréductible), la $\mathcal{A}$-dualité n'est plus équivalente à la $\mathbb{F}$-dualité de l'image q-aire. Les résultats de ce chapitre ont fait l'objet de la publication [8].

La liste des principaux symboles utilisés dans la partie II :

— $\mathbb{F} = \mathbb{F}_q$: un corps fini de cardinal q.
— $f(x)$: un polynôme unitaire de degré m sur $\mathbb{F}$.
— $\mathcal{A} = \mathbb{F}[x]/f(x)$: un quotient fini d'anneau de polynôme.
— s : la longueur des codes sur $\mathcal{A}$.
— $\mathcal{A}$-code : un code de longueur s sur $\mathcal{A}$.
— $E = \mathcal{A}^s$.
— $k = dim_{\mathbb{F}}(C)$: la dimension du $\mathcal{A}$-code C en tant que $\mathbb{F}$-espace vectoriel de E.
— $C^{\perp}$: le code dual d'un $\mathcal{A}$-code C.
— $\mathcal{C}$: le code image q-aire d'un $\mathcal{A}$-code C.
— $n = ms$: la longueur du code image q-aire $\mathcal{C}$.

Chapitre 3

Les codes sur un quotient fini d'anneau de polynômes

3.1 Notations et définitions

On considère le corps fini $\mathbb{F} = \mathbb{F}_q$, et $f(x)$ un polynôme unitaire de degré m sur $\mathbb{F}$. On construit ainsi l'anneau quotient $\mathcal{A} = \mathbb{F}[x]/f(x)$. Le $\mathbb{F}$-espace vectoriel $\{g(x) \in \mathbb{F}[x] | deg(g(x)) < m\}$ peut être identifié avec l'anneau quotient $\mathcal{A}$.

On considère dans ce chapitre des codes de longueur s définis sur $E = \mathcal{A}^s$. On réserve la lettre n pour la longueur de l'image q-aire des codes. On a alors $n = ms$.

À partir de la définition classique des codes sur les anneaux, on peut définir un $\mathcal{A}$-code comme suit :

Définition 20. *Un $\mathcal{A}$-code C de longueur s sur l'anneau $\mathcal{A}$ est un $\mathcal{A}$-sous module de E.*

Il faut noter que dans le cas d'un $\mathcal{A}$-code C, la notion de base est remplacée par celle de système de générateurs. En revanche, C est toujours un $\mathbb{F}$-sous espace vectoriel de E, ainsi on peut définir $dim_{\mathbb{F}}(C)$ comme sa dimension sur $\mathbb{F}$. En particulier, si $k = dim_{\mathbb{F}}(C)$ et $\mathbb{F} = \mathbb{F}_q$, alors $\#C = q^k$.

3.2 Matrice génératrice d'un $\mathcal{A}$-code

3.2.1 $\mathcal{A}$-matrice génératrice

On rappelle que sur un corps fini $\mathbb{F}$, une matrice génératrice G d'un code C de longueur s, est une matrice de k lignes ($k = dim(C)$), telle que ses k lignes forment une base de C sur $\mathbb{F}$.

On a vu qu'on peut associer une fonction d'encodage χ à toute matrice génératrice G :

$$\begin{array}{rccc} \chi & : & \mathbb{F}^k & \rightarrow & E \\ & & u & \mapsto & u.G \end{array}$$

Puisque G est une base de $\mathbb{F}$, on a $C = \chi(\mathbb{F}^k)$, de plus χ est injective, c'est donc une bijection de $\mathbb{F}^k$ dans C.

Dans cette section on s'intéresse aux codes sur des anneaux, en particulier ces derniers peuvent contenir des diviseurs de zéro. La notion de base n'existe plus dans cette situation, il faut se contenter de la notion de systèmes de générateurs. Dans notre travail, nous nous intéressons à des codes qui sont toujours des modules finis, il existe donc toujours au moins un système de générateurs fini.

Soit $(g^{(1)}, \ldots, g^{(k)}), g^{(i)} \in E$, pour $1 \leq i \leq k$, un système de générateurs d'un $\mathcal{A}$-code C. Si G est la matrice de taille $k \times s$ et de lignes $g^{(1)} \ldots g^{(k)}$ sur l'anneau $\mathcal{A}$. Alors l'application :

$$\begin{array}{rccc} \chi & : & \mathcal{A} & \to & E \\ & & u & \mapsto & u.G \end{array}$$

est une fonction d'encodage, avec $C = \chi(\mathcal{A}^k)$. Par contre χ n'est pas forcément injective.

La notion de dimension de C peut être remplacée par la notion du nombre minimum d'éléments k d'un système générateur de C. Même dans cette situation, l'égalité $\#C = (\#\mathcal{A})^k$, n'est pas forcément satisfaite. En particulier la fonction d'encodage n'est pas forcément injective en raison de la présence de diviseurs de 0.

Une matrice G telle que les lignes forment un système minimal de générateurs est appelée matrice génératrice du $\mathcal{A}$-code C.

En fait, la notion de nombre minimum d'éléments d'un système de générateurs n'est toujours pas satisfaisante, en particulier la fonction d'encodage n'est pas toujours injective, même avec un système minimal de générateurs.

Exemple 3. *Soit* $\mathbb{F} = \mathbb{F}_2$, $s = 3$ *et* $f(x) = (x^3 + x + 1)(x^4 + x + 1)$.
On pose

$$G = \begin{pmatrix} x^3 + x + 1 & x(x^3 + x + 1) & (x^2 + 1)(x^3 + x + 1) \\ 0 & x^4 + x + 1 & x \end{pmatrix}$$

G est une matrice génératrice d'un code C, de longueur 3.
On a :

$$Ker(\chi) = \{a(x)(x^4 + x + 1, 0) | a(x) \in \mathcal{A}\}.$$

Alors

$$\#C = 2^3 \times 2^7 \neq (\#A)^2 = (2^7)^2.$$

3.2.2 $\mathbb{F}$-matrice génératrice

La structure de $\mathcal{A}^s$, considéré comme un $\mathbb{F}$-espace vectoriel, permet de dire qu'un code C "linéaire" sur $\mathcal{A}$ ($\mathcal{A}$-linéaire), est aussi un code $\mathbb{F}$-linéaire. Ainsi le code C admet une matrice génératrice $G_{\mathbb{F}}$ sur $\mathbb{F}$ (une $\mathbb{F}$-matrice génératrice).

Soit $(g^{(1)}, \ldots, g^{(k)})$, $g^{(i)} \in E$, une base de C, vu comme un $\mathbb{F}$-espace vectoriel. On construit la matrice G de taille $k \times s$ à coefficients sur $\mathcal{A}$, et telle que

$g^{(1)}, \ldots, g^{(k)}$ sont ces lignes.
On peut définir une fonction d'encodage ϑ de $\mathbb{F}^k$ sur E par $\vartheta(b) = bG$, avec $b = (b_1, \ldots, b_k) \in \mathbb{F}^k$.
On a $C = \vartheta(\mathbb{F}^k)$, ϑ est injective et $k = dim_{\mathbb{F}}(C)$, en particulier $\#C = q^k$.

Le cas où $f(x) = x^m - 1$ et C admet un seul générateur $G = (g)$ (1-générateur), avec $g = (g_1(x), \ldots, g_s(x))$ correspond à une famille particulière de codes quasi-cycliques qui a été largement étudiée dans [39] et [40].

Dans le cas d'un $\mathcal{A}$-code C admettant un seul générateur g sur $\mathcal{A}$ ($g = (g_1(x), \ldots, g_l(x))$), on peut obtenir une matrice génératrice en tant qu'espace vectoriel sur $\mathbb{F}$ en utilisant la méthode suivante :

1. On calcule le degré d du plus grand polynôme diviseur en commun des $g_i(x)$ et $f(x)$: $d = deg(pgcd(f(x), g_1(x), \ldots, g_l(x)))$.
2. On calcule $m - d - 1$, où m est le degré de $f(x)$.
3. On forme la matrice G' génératrice de C sur $\mathbb{F}$ ($\mathbb{F}$-matrice génératrice) en prenant les lignes : $x^0 g$, xg, $\ldots x^{m-d-1} g$.

D'où la proposition :

Proposition 14. *Soit $G = (g_1(x), g_2(x), \ldots, g_s(x))$ une $\mathcal{A}$-matrice génératrice d'un $\mathcal{A}$-code C admettant un seul générateur. Le code C admet pour $\mathbb{F}$-matrice génératrice la matrice suivante :*

$$G' = \begin{pmatrix} g_1(x) & g_2(x) & \ldots & g_s(x) \\ xg_1(x) & xg_2(x) & \ldots & xg_s(x) \\ x^2 g_1(x) & x^2 g_2(x) & \ldots & x^2 g_s(x) \\ \vdots & \vdots & \vdots & \vdots \\ x^{m-d-1} g_1(x) & x^{m-d-1} g_2(x) & \ldots & x^{m-d-1} g_s(x) \end{pmatrix}$$

où $d = deg(pgcd(f(x), g_1(x), g_2(x), \ldots, g_s(x)))$.

Démonstration. On pose les notations :
— $u(x) = pgcd((f(x), g_1(x), g_2(x), \ldots, g_s(x))$.
— $v(x) = f(x)/u(x)$.
— $u_i(x) = pgcd(f(x), g_i(x))$.
— $v_i(x) = f(x)/u_i(x)$.
Il est clair que $u(x)$ divise $u_i(x)$, et que $v(x)$ est un multiple de $v_i(x)$ pour tout i. En conséquence $v(x)g_i(x) = 0 \in \mathcal{A}$, pour tout i.
Puisque un élément c de C est de la forme :

$$c = a(x)(g_1(x), \ldots, g_s(x)).$$

Et si $a(x) = q(x)v(x) + r(x)$ est la division euclidienne de $a(x)$ par $v(x)$.
Alors :

$$c = q(x)(v(x)g_1(x), \ldots, v(x)g_s(x)) + r(x)(g_1(x), \ldots, g_s(x))$$

$$= r(x)(g_1(x), \ldots, g_s(x)).$$

De plus $deg(r(x)) < m - d$, donc $c = (r_0, \ldots, r_{m-d-1})G'$.

En conséquence les lignes de G' forment un système des générateurs pour le $\mathbb{F}$-espace vectoriel C.

Montrons que G' est de rang plein. On suppose qu'il existe un $r(x) \neq 0$, tel que $deg(r(x)) < m - d$ *et* $r(x)(g_1(x), \ldots, g_s(x)) = 0$.

Autrement dit, $r(x)g_i(x) = 0 \pmod{f(x)}$ pour $1 \leq i \leq s$.

Ce qui implique que $r(x)u(x) = 0 \pmod{f(x)}$, et que $r(x)$ est divisible par $v(x)$.

Cette condition contredit le fait que $deg(r(x)) < deg(v(x))$.
En conséquence, les lignes de G' sont linéairement indépendantes et G' est une matrice $\mathbb{F}_2$-génératrice de C. □

Dans le cas général, lorsque G a plusieurs lignes, on peut construire une $\mathbb{F}$-matrice génératrice G' en remplaçant chaque ligne de G par sa matrice obtenue à l'aide de la proposition 14. Cependant cette matrice n'est en général pas de rang plein, il faudra ensuite appliquer l'élimination de Gauss pour obtenir une $\mathbb{F}$-matrice génératrice.

On reprend les données de l'exemple 3 :

Exemple 4. *Soit*

$$G = \begin{pmatrix} x^3+x+1 & x(x^3+x+1) & (x^2+1)(x^3+x+1) \\ 0 & x^4+x+1 & x \end{pmatrix}$$

une matrice génératrice d'un code C de longueur 3 sur l'anneau quotient $\mathcal{A} = \mathbb{F}_2[x]/f(x)$, tel que $f(x) = (x^3+x+1)(x^4+x+1)$.
Une $\mathbb{F}_2$-matrice génératrice de C est :

$$G' = \begin{pmatrix} x^3+x+1 & x(x^3+x+1) & (x^2+1)(x^3+x+1) \\ x^4+x^2+x & x^5+x^3+x^2 & x^6+x^3+x^2+x \\ x^5+x^3+x^2 & x^6+x^4+x^3 & x^5+x^4+1 \\ x^6+x^4+x^3 & x^4+x^3+x^2+1 & x^6+x^5+x \\ 0 & x^4+x+1 & x \\ 0 & x^5+x^2+x & x^2 \\ 0 & x^6+x^3+x^2 & x^3 \\ 0 & x^5+x^4+x^2+1 & x^4 \\ 0 & x^6+x^5+x^3+x & x^5 \\ 0 & x^6+x^5+x^4+x^3+1 & x^6 \\ 0 & x^6+x^4+x^3+x^2+x+1 & x^5+x^3+x^2+1 \end{pmatrix}$$

On peut remarquer que $dim_{\mathbb{F}_2}(C) = 11$ et que $\#C = 2^{11}$.

Nous allons maintenant présenter quelques cas particuliers.

3.2.3 Codes cycliques

Les codes cycliques correspondent au cas $s = 1$ et $f(x) = x^m - 1$. On a alors $E = \mathcal{A} = \mathbb{F}[x]/(x^m - 1)$.

Dans ce type d'anneau, tous les idéaux sont principaux, de plus il est connu dans [26], chap.7, Théorème 1, que ces codes admettent une $\mathbb{F}[x]/(x^m-1)$-matrice génératrice de type $G=(g(x))$, tel que $g(x)$ est un diviseur de $f(x)$ dans $\mathbb{F}[x]$.

L'identification d'un polynôme :

$$a(x)=\sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}[x]/(x^m-1)$$

de degré inférieur à m au m-uplet $(a_0,\ldots,a_{m-1})$ de ces coefficients revient à passer de la $\mathcal{A}$-matrice génératrice $G=(g(x))$ à la matrice canonique de ce code cyclique en utilisant la proposition 14.

Cette correspondance sera détaillée dans la section 4.1.

Exemple 5. *Soit $\mathbb{F}_2[x]/(x^7-1)$, si C est un $\mathcal{A}$-code, de matrice génératrice $G=(x^3+x+1)$, alors :*

$$G'=\begin{pmatrix} x^3+x+1 \\ x^4+x^2+x \\ x^5+x^3+x^2 \\ x^6+x^4+x^3 \end{pmatrix}$$

Sur $\mathbb{F}_2$:

$$G'_{\mathbb{F}_2}=\begin{pmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \end{pmatrix}.$$

3.2.4 Codes consta-cycliques

Un code consta-cyclique est un code qui reste invariant si on lui applique une permutation circulaire suivie d'une multiplication par un scalaire $a\in\mathbb{F}^*$ sur sa première composante.

Les codes constat-cycliques correspondent en fait aux $\mathcal{A}$-codes de longueur $s=1$, tels que $\mathcal{A}=\mathbb{F}[x]/f(x)$ avec $f(x)=x^m-a$, pour $a\in\mathbb{F}^*$.

3.2.5 Codes quasi-cycliques

Les codes quasi-cycliques correspondent au cas $f(x)=x^m-1$ et $s\geq 1$. Cette approche est classique, et elle a été utilisée dans [25] et [23].

Les codes quasi-cycliques classiques sur le corps fini $\mathbb{F}$ sont obtenus en remplaçant chaque ligne de longueur s de sa $\mathbb{F}$-matrice génératrice donnée dans la proposition 14, par une ligne de longueur ms, composée des coefficients des polynômes de la ligne.

3.2.6 Codes sur des extensions du corps $\mathbb{F}$

Si $f(x)$ est un polynôme irréductible sur $\mathbb{F}$, $\mathcal{A} = \mathbb{F}[x]/f(x)$ est alors une extension K de degré m du corps fini $\mathbb{F}$ ($\mathcal{A} = \mathbb{F}_{q^m}$). Les $\mathcal{A}$-codes sont dans ce cas les codes K-linéaires. Dans cette situation, tous les résultats présentés dans cette section sont plus ou moins triviaux.

3.3 Dualité des $\mathcal{A}$-codes

Soient $u = (u_1(x), u_2(x), \ldots, u_s(x))$ et $v = (v_1(x), v_2(x), \ldots, v_s(x))$, deux éléments de E. On définit le produit scalaire sur E comme suit :

$$< u, v >= \sum_{i=1}^{s} u_i(x)v_i(x) \in \mathcal{A}.$$

Ce produit scalaire est une forme $\mathcal{A}$-bilinéaire symétrique sur E, dans le sens que, pour u, $v \in E$ et $a(x)$, $b(x) \in \mathcal{A}$,

$$< a(x)u + b(x)u', v >= a(x) < u, v > +b(x) < u', v >$$

et

$$< u, v >=< v, u > .$$

On note que cette forme bilinéaire est non-dégénérée, c'est-à-dire que, si pour tout $v \in E$, $< u, v >= 0$, alors $u = 0$. On peut aussi remarquer que ce produit scalaire est $\mathbb{F}$-bilinéaire, mais à valeur dans $\mathcal{A}$.

On définit alors le dual d'un $\mathcal{A}$-code de manière similaire au cas des codes $\mathbb{F}$-linéaires :

$$C^{\perp} = \{v \in E | < u, v >= 0, \ \forall u \in C\}.$$

En tenant compte des remarques précédentes sur cette forme bilinéaire non-dégénérée, on obtient les propriétés suivantes :

Proposition 15. *1. Le code dual $C^{\perp}$ de C est aussi un $\mathcal{A}$-code.*

2. Si $(g^{(1)}, \ldots, g^{(k)})$ est un système de générateurs du $\mathcal{A}$-code C, alors son code dual est l'ensemble

$$C^{\perp} = \{v \in E | < g^{(i)}, v >= 0, \ \forall i = 1, \ldots, k\}.$$

3. Si G est une matrice génératrice associée à $(g^{(1)}, \ldots, g^{(k)})$, alors

$$C^{\perp} = \{v \in E | Gv^t = 0\}.$$

4. Si $dim_{\mathbb{F}}(C)$ est la dimension de C en tant que $\mathbb{F}$-espace vectoriel, alors $dim_{\mathbb{F}}(C^{\perp}) = sm - dim_{\mathbb{F}}(C)$, exprime la dimension sur $\mathbb{F}$, du code $C^{\perp}$.

Démonstration.

1. Les éléments de $C^{\perp}$, sont des éléments de E, et la forme bilinéaire non dégénérée du produit scalaire fait de $C^{\perp}$ un $\mathcal{A}$-sous module de E.
2. Évident.
3. D'après 2.
4. $C^{\perp}$ est le $\mathbb{F}$-sous espace orthogonal à C, alors $sm = dim_{\mathbb{F}}(C^{\perp}) + dim_{\mathbb{F}}(C)$, d'où $dim_{\mathbb{F}}(C^{\perp}) = sm - dim_{\mathbb{F}}(C)$.

□

3.4 Matrice génératrice canonique

L'objectif de cette section est de définir une matrice canonique pour les $\mathcal{A}$-codes. Cette matrice sera dérivée de la forme d'Hermite des matrices [45]. Il faudra ensuite introduire une réduction supplémentaire pour obtenir l'unicité.

3.4.1 Forme d'Hermite

Une matrice G à coefficients dans $\mathcal{A}$ est dite sous forme d'Hermite si elle vérifie les conditions suivantes :

— G est une matrice échelonnée.
— Les premiers polynômes non nuls de chaque ligne sont des diviseurs de $f(x)$.
— Si $g_{i,j}$ est le premier polynôme non nul d'une ligne i, alors $deg(g_{t,j}) < deg(g_{i,j})$ pour $t < i$.

Exemple 6. *Soit $\mathbb{F} = \mathbb{F}_2$, et $f(x) = (x^3 + x + 1)(x^4 + x + 1)$. On considère le $\mathcal{A}$-code C, généré par la matrice :*

$$G_1 = \begin{pmatrix} x^4 + x + 1 & 1 \end{pmatrix}.$$

Cette matrice satisfait les conditions données ci-dessus.

Pour monter que ces conditions ne sont pas suffisantes pour avoir l'unicité, on considère la deuxième matrice G_2 définie par :

$$G_2 = \begin{pmatrix} x^4 + x + 1 & 1 \\ 0 & x^3 + x + 1 \end{pmatrix}$$

Cette matrice est aussi une matrice génératrice du $\mathcal{A}$-code C, et elle est bien sous la forme d'Hermite. La deuxième ligne de G_2 génère un sous-code $C^{(2)}$ particulier de C. En effet, si $c = (c_1(x), c_2(x)) \in C$ et $c_1(x) = 0$, alors c est un mot de $C^{(2)}$. Cette remarque va être étudiée en détail dans la suite et permettra d'obtenir une forme canonique.

La matrice binaire correspondant à G_2 est alors :

$$G_{\mathbb{F}_2} = \left(\begin{array}{c|c} 1\,1\,0\,0\,1\,0\,0 & 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,1\,0 & 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,1 & 0\,0\,1\,0\,0\,0\,0 \\ \hline 0\,0\,0\,0\,0\,0\,0 & 1\,1\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 & 0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,1\,1\,0\,1 \end{array}\right)$$

On remarque que les blocs diagonaux de cette matrice binaire correspondent à des matrices canoniques de codes cycliques.

3.4.2 Pseudo division et ordre partiel sur E

On introduit dans ce paragraphe une notion d'ordre partiel sur E. Il s'agit en fait d'un cas particulier d'ordre partiel utilisé dans la théorie des bases de Gröbner, mais nous n'utiliserons ici que la division euclidienne qui est suffisante dans le contexte des $\mathcal{A}$-codes.

Notation 1. *Soit $e = (e_1(x), \ldots, e_s(x))$ un élément de E. On note par :*
- *$L_{ind}(e)$ ("premier indice"), le plus petit indice i de e tel que $e_i(x) \neq 0$.*
- *$L_{coef}(e) = e_{L_{ind}(e)}(x)$ ("premier coefficient"), le premier polynôme non nul de e.*

Par convention pour $e = 0$, on pose $L_{ind}(0) = s + 1$ et $L_{coef}(0) = 0$.

Proposition 16. *Soient $e = (e_1(x), \ldots, e_s(x))$ un élément non nul de E, $i = L_{ind}(e)$ son premier indice, et $g(x) = L_{coef}(e)$ son premier coefficient.*

Si $a(x)g(x)+b(x)f(x) = d(x)$ est l'identité de Bézout relative à $g(x)$ et $f(x)$ dans $\mathbb{F}[x]$, et $d(x)$ est unitaire, alors $e' = a(x)e$ est appelé la normalisation de e dans E. Et puisque $a(x)$ et $f(x)$ sont premiers entre eux, nous avons :
- *$d(x)$ est un diviseur de $f(x)$, $deg(d(x)) \leq deg(g(x))$.*
- *$L_{ind}(e) = L_{ind}(e')$, $L_{coef}(e') = d(x)$.*
- *e et e', génèrent le même $\mathcal{A}$-module de E.*

On note que cette normalisation est à priori définie à multiplication scalaire près par un élément $\kappa \in \mathbb{F}^*$. C'est la condition sur $d(x)$ unitaire qui garantit l'unicité de cette normalisation.

Les notions de "premier indice" et "premier coefficient" se généralisent à un $\mathcal{A}$-code C de la manière suivante :

Définition 21. *Soit C un $\mathcal{A}$-code, le "premier indice" $L_{ind}(C)$ de C est le minimum des "premiers indices" de ses mots c_i.*
Le "premier coefficient" $L_{coef}(C)$ de C, est le seul polynôme unitaire $g(x)$ qui satisfait les conditions suivantes :

1. *Il existe un mot c_i dans C tel que $L_{ind}(c_i) = L_{ind}(C)$ et $L_{coef}(c_i) = g(x)$.*
2. *Le degré de $g(x)$ est minimal parmi tous les polynômes qui satisfassent la première condition.*

On désigne par le "premier élément" d'un code C le mot c, tel que : $L_{ind}(c) = L_{ind}(C)$ et $L_{coef}(c) = L_{coef}(C)$.

La conséquence directe de l'application de la normalisation de la proposition 16 sur le premier élément d'un code C, est le fait que le "premier coefficient" $L_{coef}(C)$ non nul du code est toujours un diviseur de $f(x)$.

Définition 22. *Soient $u = (u_1(x), \ldots, u_s(x))$ et $v = (v_1(x), \ldots, v_s(x))$ deux éléments de E.*
On dit que u est "plus grand ou égal" que v, et on note $u \succeq v$, si le "premier indice" de u est strictement plus grand que le "premier indice" de v : $L_{ind}(u) > L_{ind}(v)$, ou bien si $L_{ind}(e) = L_{ind}(v)$ et $deg(L_{coef}(e)) \geq deg(L_{coef}(v))$.

On note que cette relation est transitive, mais n'est pas anti-symétrique.

Exemple 7. *Soient $u = (0, 0, x^5 + 1, x^2)$ et $v = (0, 0, x^4 + x, x)$, alors $u \succeq v$.*

A ce stade d'étude, on est capable de définir la notion de "pseudo-division" sur E :

Définition 23. *Soient $u = (u_1(x), \ldots, u_s(x))$ et $v = (v_1(x), \ldots, v_s(x))$ deux éléments de E, avec $u \neq 0$, on pose $i = L_{ind}(u)$.*
On considère la division euclidienne de $v_i(x)$ par $u_i(x)$:

$$v_i(x) = q(x)u_i(x) + r(x),\ deg(r(x)) < deg(u_i(x)).$$

"La pseudo-division" de v par u est la relation suivante :

$$v = q(x)u + w.$$

Le polynôme $q(x)$, est appelé "le quotient" de v par u : $q(x) = quo(v, u)$.
L'élément $w = v - q(x)u \in E$, est appelé "le reste" de v par u : $w = rem(v, u)$.

À partir de cette définition, on a les propriétés suivantes :

Lemme 2.
- *Si $v \prec u$, alors $quo(v, e) = u$ et $rem(v, u) = v$.*
- *Si $L_{ind}(v) = L_{ind}(u)$ alors $rem(v, u) \prec u$.*

3.4.3 Base de diviseurs d'un $\mathcal{A}$-code

Notre but est de construire un ensemble ordonné de générateurs $(g^{(1)}, \ldots, g^{(k)})$ d'un $\mathcal{A}$-code C, afin de généraliser les propriétés des générateurs canoniques des codes cycliques rappelées ci-dessous :

1. Si C est un code cyclique généré par $g(x)|(x^m - 1)$, alors $a(x) \in C$ si et seulement si $a(x) = 0 \bmod g(x)$.
2. Si $m(x)$ est le quotient de $a(x)$ par $g(x)$ dans $\mathbb{F}[x]$, alors $a(x) = m(x)g(x) \pmod{x^m - 1}$, c'est-à-dire que $a(x) = m(x)g(x)$ dans $\mathcal{A}$.

Si c est un élément quelconque de E, on veut que notre système de générateurs $(g^{(1)}, \ldots, g^{(k)})$ vérifie les propriétés suivantes :

Si on calcule les quotients successifs $q_i(x) \in \mathcal{A}$, et les restes successifs $r^{(i)} \in E$ de c par les $g^{(i)}$, alors

1. c est un élément de C si et seulement $r^{(k)} = 0 \in E$.
2. Si $c \in C$, alors $c = \sum_{i=1}^{k} q_i(x) g^{(i)}$.

On introduit pour cela certains $\mathcal{A}$-sous codes de C. Pour $i = 1, \ldots, s+1$, on pose :

$$C_i = \{c \in C | L_{ind}(c) \geq i\}.$$

On a par exemple $C_1 = C$, $C_2 = \{c = (c_1|c_2|\ldots|c_s) \in C | c_1 = 0\}$, et ainsi de suite jusqu'à $C_{s+1} = \{0\}$.

On obtient ainsi une séquence décroissante de $\mathcal{A}$-sous-codes de C :

$$C_1 = C \supseteq C_2 \supseteq C_3 \ldots \supseteq C_{s+1} = \{0\}. \tag{3.1}$$

Soit $k+1$ le nombre des sous-codes distincts de cette section. On ne veut garder que les sous-codes distincts ordonnés. Pour cela, on note par $(i_1, i_2, \ldots, i_k)$ la séquence ordonnée de ces indices :

$$i_1 = max\{j | C_j = C_1\},$$

$$i_2 = max\{j | C_j = C_{i_1+1}\},$$

$$\vdots$$

$$i_k = max\{j | C_j = C_{i_{k-1}+1}\}.$$

Par construction, puisque $C_{s+1} = \{0\}$, alors $C_j = \{0\}$ pour $i_k < j \leq s+1$. On définit les sous-codes $C^{(j)} = C_{i_j}$ pour $j \in [1, k]$ et $C^{(k+1)} = \{0\}$. On a ainsi construit une séquence décroissante de sous-codes de C :

$$C = C^{(1)} \supsetneq C^{(2)} \supsetneq C^{(3)} \ldots \supsetneq C^{(k)} \supsetneq \{0\} = C^{(k+1)}. \tag{3.2}$$

Par construction : $L_{ind}(C^{(j)}) = i_j$.

Le lemme suivant est une étape très importante dans la construction de la base de diviseurs.

Lemme 3. *Soit $g^{(j)}$ le "premier élément" de $C^{(j)}$, pour $1 \leq j \leq k$. On a*

$$C^{(j)} = \{h(x)g^{(j)} + c^{(j+1)} \mid c^{(j+1)} \in C^{(j+1)}, h \in \mathcal{A}, deg(h) < m - deg(L_{coef}(g^{(j)})\}.$$

Démonstration. Soit c un élément de $C^{(j)}$, on pose :

— $i = L_{ind}(C^{(j)})$.
— $h(x) = quo(c, g^{(j)})$.
— $c' = rem(c, g^{(j)})$.

Selon la définition de la pseudo division, $deg(h(x)) < m - deg(L_{coef}(g^{(j)}))$ et $c' < g^{(j)}$.

Notons que, pour $c' \in C^{(j)}$, si $c'_i(x) \neq 0$, alors $L_{ind}(c') = L_{ind}(C)$ et $deg(c'_i(x)) < deg(L_{coef}(g^{(j)}))$. Cela contredit le fait que $g^{(j)}$ est le "premier élément" de $C^{(j)}$. Alors $c'_i(x) = 0$ et $c' \in C^{(j+1)}$.

□

À ce stade d'étude, on est capable de démontrer le résultat principal de cette section :

Théorème 10. *Soit $(g^{(1)}, \ldots, g^{(k)})$ l'ensemble ordonné des premiers éléments des codes $C^{(1)}, C^{(2)}, \ldots, C^{(k)}$. Un élément c de E est un mot de C, si et seulement s'il existe un unique $k-uplet$: $(h_1(x), \ldots, h_k(x)) \in \mathcal{A}^k$, tel que $deg(h_j(x)) < m - deg(L_{coef}(g^{(j)})$, avec $1 \leq j \leq k$ et $c = \sum_{j=1}^{k} h_j(x)g^{(j)}$.*

Démonstration. Soit c un élément de E. On applique à c l'algorithme de divisions successives par $(g^{(1)}, \ldots, g^{(k)})$:

Algorithme 1 Division par l'ensemble des "premiers éléments" de la base de diviseurs

Entrées : $c \in \mathcal{A}^s$, et $(g^{(1)}, \ldots, g^{(k)})$ (premiers éléments de $C^{(1)}, \ldots C^{(k)}$)
Sorties : $(h_1(x), \ldots, h_k(x)) \in \mathcal{A}^k$ et $r \in E$ tels que
$deg(h_j(x)) < m - deg(L_{coef(g^{(j)})})$ et $c = \sum_{j=1}^{k} h_j(x)g^{(j)} + r$

Initialisation : $r := c$
Pour $j := 1$ à k **faire** :
$h_j(x) := quo(r, g^{(j)})$
$r := rem(r, g^{(j)})$
Fin pour
Retourner $(h_1(x), \ldots, h_k(x))$ et r

On a $c = \sum_{j=1}^{k} h_j(x)g^{(j)} + r$, et puisque $(g^{(1)}, \ldots, g^{(k)})$ sont des éléments de C alors $c \in C$ si et seulement si $r \in C$. Mais étant donné que par construction, $r \notin C^{(k)}$, on a bien $c \in C$ si et seulement si $r = 0$.

On suppose que $c \in C$, selon le lemme 3, $c = \sum_{j=1}^{k} h_j(x)g^{(j)} \in C$.

Montrons maintenant que cette décomposition est unique :
Supposons qu'il existe deux k-uplets $(h_1(x), \ldots, h_k(x))$ et $(h'_1(x), \ldots, h'_k(x))$ distincts dans E, et tels que $c = \sum_{j=1}^{k} h_j(x)g^{(j)} = \sum_{j=1}^{k} h'_j(x)g^{(j)}$.
On choisit i le plus grand indice tel que $h_i(x) \neq h'_i(x)$.
Il est clair que, $(h'_i(x) - h_i(x))g^{(i)} = \sum_{j=i+1}^{k}(h_j(x) - h'_j(x))g^{(j)} \in C^{(i+1)}$, avec $deg((h'_i(x) - h_i(x))g^{(i)}) < m$. Le seul cas possible est $h'_i(x) - h_i(x) = 0$, ce qui est en contradiction avec l'hypothèse.
En conséquence cette décomposition est unique.

□

On note que la matrice $G_2 = \begin{pmatrix} x^4+x+1 & 1 \\ 0 & x^3+x+1 \end{pmatrix}$ de l'exemple 6 correspond à une base de diviseurs de C, contrairement à la matrice
$G_1 = \begin{pmatrix} x^4+x+1 & 1 \end{pmatrix}$

Définition 24. *Soit $B = (g^{(1)}, g^{(2)}, \ldots, g^{(k)})$, un k-uplets de E, B est une base de diviseurs du code C si les $g^{(i)}$ forment une séquence ordonnée des "premiers éléments" des codes $C^{(1)}, \ldots, C^{(k)}$.*

La proposition suivante est une conséquence directe du théorème 10 :

Proposition 17.
Soit C un $\mathcal{A}$-code, et $(C^{(1)}, \ldots, C^{(k)})$ la séquence strictement décroissante des sous-codes de C, décrite dans 3.4.3. Le cardinal de toute base de diviseurs $B = (g^{(1)}, g^{(2)}, \ldots, g^{(k)})$ du code C est k. En outre si $r_i = deg(L_{coef}(g^{(i)}))$, alors r_i est indépendant du choix de la base des diviseurs, et $\#C = q^{k'}$ avec $k' = \sum_{i=1}^{k}(m - r_i)$.

Démonstration. À partir de la définition du "premier élément ", on sait que le choix du polynôme unitaire est décisif dans la définition du "premier élément" d'un code $C^{(i)}$, le "premier coefficient" de ce "premier élément" ne dépend pas du choix du "premier élément" lui même.
En ce qui concerne l'égalité : $\#C = q^{k'}$ avec $k' = \sum_{i=1}^{k}(m - r_i)$, on la déduit à partir de la contrainte posée sur $h_i(x)$, et de l'unicité de la décomposition du théorème 10. □

Notation 2. *Soit $B = (g^{(1)}, \ldots, g^{(k)})$, on note :*
- *$Liste_{coef}(B) = (L_{coef}(g^{(1)}), \ldots, L_{coef}(g^{(k)}))$.*
- *$Liste_{deg}(B) = (deg(L_{coef}(g^{(1)})), \ldots, deg(L_{coef}(g^{(k)})))$.*
- *$Liste_{ind}(B) = (L_{ind}(g^{(1)}), \ldots, L_{ind}(g^{(k)}))$.*

Lemme 4. *Soient $B = (g^{(1)}, \ldots, g^{(k)})$ et $B' = (g'^{(1)}, \ldots, g'^{(k)})$, deux bases de diviseurs d'un code C, on a :*
- *$Liste_{coef}(B) = Liste_{coef}(B')$.*
- *$Liste_{deg}(B) = Liste_{deg}(B')$.*
- *$Liste_{ind}(B) = Liste_{ind}(B')$*

Démonstration. Soient $g^{(j)} \in B$ et $g'^{(j)} \in B'$, avec $j \in [1, \ldots, k]$. D'après le lemme 3 $g^{(j)} = h(x)g'^{(j)} + c^{(j+1)}$, ainsi $deg(L_{coef}(g'^{(j)})) \leq deg(L_{coef}(g^{(j)}))$ (1).

On a aussi
$g'^{(j)} = h'(x)g^{(j)} + c^{(j+1)}$ et alors $deg(L_{coef}(g^{(j)})) \leq deg(L_{coef}(g'^{(j)}))$ (2).

On déduit de (1) et (2) l'égalité $deg(L_{coef}(g'^{(j)})) = deg(L_{coef}(g'^{(j)}))$, et puisque $L_{coef}(g^{(j)})$ et $L_{coef}(g'^{(j)})$ sont unitaire alors $h(x) = h'(x) = 1$. □

Lemme 5. *Soit $(g^{(1)}, \ldots, g^{(k)})$ une base de diviseurs d'un code C, alors les $L_{coef}(g^{(i)})$ sont des diviseur de $f(x)$, pour $1 \leq i \leq k$.*

Démonstration. Soit $g^{(i)}$ un élément de la base des diviseurs, avec $i \in [1, \ldots, k]$, et $p_i(x) = L_{coef}(g^{(i)})$. On pose $\lambda(x) = pgcd(p_i(x), f(x))$, alors il existe $\alpha(x), \beta(x) \in \mathcal{A}$ tels que : $\alpha(x)p_i(x) + \beta(x)f(x) = \lambda(x)$, avec $deg(\lambda(x)) \leq deg(p_i(x))$ (1).
Si on multiplie par $\alpha(x)$ l'élément $g^{(i)}$ alors : $\alpha(x)g^{(1)} = (0, \ldots, 0, \lambda(x), \ldots)$ et alors $deg(p_i(x)) \leq deg(\lambda(x))$ (2).

D'après (1) et (2) on peut conclure que $\lambda(x) = p_i(x)$.

Alors pour tout $i \in [1, \ldots, k]$ le $L_{coef}(g^{(i)})$ est un diviseur de $f(x)$. □

3.4.4 Base canonique de diviseurs

Pour un $\mathcal{A}$-code donné, il existe plusieurs bases de diviseurs. Dans [23] les auteurs introduisent une base canonique pour un code quasi-cyclique en utilisant les bases de Gröbner. En appliquant une approche plus directe évitant le recours aux bases de Gröbner, nous avons généralisé leur résultat pour $f(x)$ unitaire quelconque.

L'algorithme ci-dessous permet la normalisation de toute base de diviseurs B, afin de la rendre canonique.

Algorithme 2 Réduction d'une base de diviseurs.

Entrées : $B = (g^{(1)}, \ldots, g^{(k)})$, une base de diviseurs de C.
Sorties : Une base de diviseurs réduite.
Pour $j := 2$ à k faire :
Pour $i := 1$ à $j - 1$ faire :.
$g^{(i)} := rem(g^{(i)}, g^{(j)})$.
Fin pour
Fin pour
Retourner $(g^{(1)}, \ldots, g^{(k)})$.

Théorème 11. *Soit B une base de diviseurs d'un $\mathcal{A}$-code C. Si B' est la base réduite de B obtenue à l'aide de l'algorithme 2, alors B' est une base de diviseurs de C. Si G' est la matrice génératrice du code C dont les lignes sont les éléments de B', alors*

1. *G' est sous forme échelonnée.*
2. *Tous les "premiers coefficients" des lignes sont des diviseurs unitaires de $f(x)$.*
3. *Si $g_{i,j}$ est le premier coefficient de la $i$ème ligne, alors $deg(g_{t,j}) < deg(g_{i,j})$ pour tout $t < i$.*

Démonstration. Le fait que B' est une base de diviseurs de C, vient du fait que l'opération $g^{(i)} = rem(g^{(i)}, g^{(j)})$ pour $i < j$, n'affecte pas le fait que $g^{(i)}$ est le "premier élément" de $C^{(i)}$, chose qui implique directement 1 et 2. La condition 3 est une conséquence directe de la réduction $g^{(i)} = rem(g^{(i)}, g^{(j)})$, pour $i < j$. □

Proposition 18. *Si C est un $\mathcal{A}$-code admettant une matrice G' dont les lignes forment une base de diviseurs, et telle que G' satisfasse les trois conditions précédentes du théorème 11, alors G' est unique. Autrement dit, la base de diviseurs réduite d'un code est unique.*

Démonstration. Soient B et B' deux bases réduites de diviseurs de C, avec $g^{(j)} \in B$ et $g'^{(j)} \in B'$, pour $j \in [1, \ldots, k]$. D'après 3.4.3, $g^{(j)} = h(x)g'^{(j)} + c^{(j+1)}$, et $h(x) = 1$, alors $g^{(j)} - g'^{(j)} = c^{(j+1)}$, et alors $g^{(j)}_{j+1}(x) - g^{('j)}_{j+1}(x) = c_{i_{j+1}}(x)$, et puisque B est une base réduite alors d'après la troisième condition du théorème 11

$$deg(g^{(j)}_{j+1}(x)) < deg(L_{coef}(c^{(j+1)}))$$

de la même manière :

$$deg(g^{('j)}_{j+1}) < deg(L_{coef}(c^{(j+1)}))$$

Ainsi :

$$deg(g^{(j)}_{j+1}(x) - g^{('j)}_{j+1}(x)) < deg(L_{coef}(c^{(j+1)}(x)))$$

Alors

$$deg(c_{i_{j+1}}(x)) < deg(L_{coef}(c^{(j+1)}))$$

Ce qui se contredit la définition du "premier élément". On a alors $L_{coef}(c^{(j+1)}) = 0$, et ainsi $B = B'$ par induction. □

Définition 25. *La base de diviseurs B, qui satisfait les conditions du théorème 11 est appelée la base canonique de diviseurs du code C. Sa matrice associée est appelée la matrice génératrice canonique du $\mathcal{A}$-code C.*

3.4.5 Construction d'une base de diviseurs canonique

On présente en détail dans cette section la méthode de construction d'une base de diviseurs canonique d'un $\mathcal{A}$-code C à partir d'une matrice génératrice G, c'est-à-dire à partir d'un système de générateurs $(g^{(1)}, \ldots, g^{(s)})$. A priori, s n'est pas toujours égal à k (le nombre de sous-codes décrits dans l'équation 3.2).

L'algorithme 3 ci-dessous, prend en entrée un système de générateur du code $C^{(i)}$ et retourne le "premier élément" de $C^{(i)}$ ainsi qu'un système de générateur de $C^{(i+1)}$ (une liste vide si $C^{(i+1)} = \{0\}$) permettant ainsi de réitérer le processus.

Algorithme 3 Calcul du premier élément d'un code $C^{(i)}$ et génération d'un système de générateurs de $C^{(i+1)}$

Entrées : : $B = (g^{(1)}, \ldots, g^{(s)}) \neq \emptyset$, un système de générateurs d'un code $C^{(i)}$.

Sorties : : Le "premier élément" g du code $C^{(i)}$, et un système de générateur B_2, du code $C^{(i+1)}$ (B_2 peut être égal à l'ensemble vide).

1 : $j := min\{L_{ind}(g^{(i)}) | i \in [1, \ldots, s]\}$.
2 : $B_1 := \emptyset, B_2 := \emptyset$.
3 : **Pour** $i := 1$ à s faire :
4 : **Si** $L_{ind}(g^{(i)}) = j$ alors :
5 : Ajouter $g^{(i)}$ à B_1
6 : **Sinon**
7 : Ajouter $g^{(i)}$ à B_2
8 : **Finsi**
9 : **Fin pour**
10 :**Pour** $g^{(i)}$ dans B_1 faire :
11 : **On calcule** $a(x)$ **tel que :**
$L_{coef}(g^{(i)})a(x) := PGCD(f(x), L_{coef}(g^{(i)}))$
12 : $g^{(i)} := a(x)g^{(i)}$
13 :**Fin pour**
14 : $d(x) := pgcd(L_{coef}(g^{(i)}) | g^{(i)} \in B_1)$
15 : Calculer les ι_j (relation de Bézout $d(x) = \sum_{g^{(i)} \in B_1} \iota_j L_{coef}(g^{(i)})$)
16 : $g := \sum_{g^{(i)} \in B_1} \iota_j g^{(i)}$
17 :**Pour tout** $g^{(i)}$ dans B_1 faire :
18 : $g'^{(i)} := rem(g^{(i)}, g)$
19 : **Si** $g'^{(i)} \neq 0$ alors :
20 : Ajouter $g'^{(i)}$ à B_2
21 : **Finsi**
22 :**Fin pour**
23 : $h(x) := f(x)/d(x)$
24 : $g' := h(x)g$
25 :**Si** $g' \neq 0$ alors :
26 : Ajouter g' à B_2
27 :**Finsi**
28 :**Fin pour**
29 :**Retourner** g et B_2.

Proposition 19. *Soit $B = (g^{(1)}, \ldots, g^{(s)}) \neq \emptyset$, le système des générateurs de $C^{(i)} \neq \{0\}$ donné en entrée de l'algorithme 3.*

La première sortie g de l'algorithme est le "premier élément" de $C^{(i)}$. La deuxième sortie est un système de générateurs B_2 de $C^{(i+1)}$ (ou l'ensemble vide si $C^{(i+1)} = \{0\}$).

De plus, la valeur j de la ligne "1" de l'algorithme est le plus grand entier tel que $C^{(i)} = C_j$ (selon les relations de 3.1 et 3.2).

Démonstration. La dernière remarque sur j vient directement des définitions de $C^{(i)}$ et C_j.

Pour démontrer l'algorithme on regarde dans les détails ses lignes :

— 1 à 9 : $B_2 = \{g \in B / g \in C^{(i+1)}\}$, $B_1 = \{g \in B / g \notin B_2\}$

— 10 à 13 : normalisation qui assure que les premiers coefficients des éléments de B_1 sont des diviseurs de $f(x)$, autrement dit, pour $g \in B_1$, $L_{coef}(g)|f(x)$.

— 14 à 16 : la valeur de g fait de lui un élément de $C = C^{(i)}$, et tel que $L_{ind}(g) = L_{ind}(C)$, de plus $d(x) = L_{coef}(g)$ est un diviseur de $f(x)$. Ainsi g est bien le "premier élément" de C.

— 17 à 22 : C est généré par $\{g\} \cup B_2$. Les éléments ajoutés dans B_2 sont de $C^{(i+1)}$.

— 23 à 27 : on ajoute à B_2 l'élément $g' = (f(x)/d(x))g$ de $C^{(i+1)}$.

Après s'être assurer que tous les éléments de B_2 sont dans $C^{(i+1)}$, il reste à monter que B_2 est un système des générateurs de $C^{(i+1)}$.

À la ligne 22, l'union $\{g\} \cup B_2$ est un système de générateurs de C, tel que tout élément de C est de la forme $c = a(x)g + \sum_{g^{(i)} \in B_2} \iota_i g^{(i)}$. On peut clairement voir que $\sum_{g^{(i)} \in B_2} \iota_i g^{(i)}$ est un élément de $C^{(i+1)}$. Alors c est dans $C^{(i+1)}$ si et seulement si, $a(x)L_{ceof}(g) = q(x)d(x) = 0 \ mod(f(x))$. Autrement dit, $a(x)$ est un multiple de $h(x)$ et $c = a'(x)g' + \sum_{g^{(i)} \in B_2} \iota_i g^{(i)}$, avec $a'(x) = a(x)/h(x)$. □

Par conséquent, on est capable de calculer la base réduite des diviseurs d'un $\mathcal{A}$-code C, à partir d'une base de générateurs G de la manière suivante :

1. On applique l'algorithme 3 à un système de générateurs G du code C. On obtient les "premiers éléments " $g^{(1)}, g^{(2)}, \ldots, g^{(k)}$ des codes $C = C^{(1)}$, $C^{(2)}$,...,$C^{(k)}$, tels qu'ils vont être obtenues récursivement. Ainsi qu'un système de générateurs de $C^{(2)}$,...,$C^{(i)} = \{0\}$.
2. En appliquant l'algorithme 2 à la base des diviseurs obtenue à l'aide de l'algorithme 3.4.4, on calcule la base réduite des générateurs de C.

Exemple 8. *La matrice canonique, associée à la base réduite du premier exemple de ce chapitre est :*

$$G' = \begin{pmatrix} x^3+x+1 & x^2+1 & 1 \\ 0 & x^4+x+1 & x \\ 0 & 0 & x^3+x+1 \end{pmatrix}$$

On peut remarquer que le nombre de lignes de la matrice canonique du code n'est pas invariant par permutation. Si on permute les colonnes 1 *et* 2*, alors la matrice réduite est :*

$$G' = \begin{pmatrix} 1 & x^2+x+1 & x^5+x^3+x^2 \\ 0 & x^3+x+1 & x^6+x^4+0 \end{pmatrix}.$$

3.5 Système générateur du dual d'un $\mathcal{A}$ code

Si $(g^{(1)}, \ldots, g^{(k)})$ est un système de générateurs d'un $\mathcal{A}$-code C, on a vu que le dual est l'ensemble des $h \in \mathcal{A}$, tels que $< h, g^{(i)} >= 0$, pour $i \in [1, \ldots, k]$. Un des objectifs est de construire efficacement un système de générateurs pour son dual.

Le but de cette section est de généraliser le résultat ci-dessous, bien connu dans le cas linéaire.

Soit I_k la matrice identité, si $G = (I_k|B)$ est la matrice systématique d'un code linéaire C, alors la matrice $H = (-B^T|I_{s-k})$ est une matrice génératrice du code dual $C^\perp$ [[26] chap. 1 et 2].

Ce résultat est directement vérifiable si la base réduite des diviseurs d'un $\mathcal{A}$-code est sous une forme systématique, autrement dit, si tous les "premiers coefficients" sont égaux à 1, et $C^{(i)} = C_i$ pour tout $i \in [1, \ldots, s+1]$, comme défini dans la section 3.4.3.

Plus généralement, lorsque la matrice est échelonnée, et si le premier coefficient de chaque ligne est égal à 1, alors il suffit de permuter quelques coefficients afin de pouvoir appliquer la méthode.

Dans le cas général, lorsque le "premier coefficient" est de degré supérieur à 0, alors l'application de la méthode ci-dessus s'avère plus compliquée.

Pour simplifier, on suppose que le "premier indice" est égal à 1. Dans ce cas on a $C = C_1 = C^1 \supsetneq C_2 = C^{(2)}$.

Dans [8], théorème 3, nous avons proposé une construction d'une matrice génératrice du code dual $C^\perp$. Malheureusement cette construction ne prenait pas en considération quelques cas particuliers. Dans [32], A. Niksereth a donné un contre exemple de cette construction et a apporté la modification nécessaire pour obtenir la bonne forme de la matrice génératrice du dual. C'est cette dernière version corrigée que nous présentons ici.

Soit C un $\mathcal{A}$-code de longueur s, tel que son premier indice est 1. on note $g^{(1)} = (g_{1,1}(x), \ldots, g_{1,s}(x))$ "le premier élément" de la base des diviseurs. On note par C' le code poinçonné de $C^{(2)}$ sur la première position, c'est-à-dire en enlevant la première coordonnée nulle des éléments de $C^{(2)}$. Si G' est la matrice canonique de C', la matrice canonique G de C est :

$$G = \left(\begin{array}{c|ccc} g_{1,1}(x) & g_{1,2}(x) & \ldots & g_{l,s}(x) \\ \hline 0 & & & \\ \vdots & & G' & \\ 0 & & & \end{array}\right).$$

On pose $h_{1,1} = f(x)/g_{1,1}(x)$. On note par $H' = (h'_{i,j}(x))$, pour $2 \leq i, j \leq s$ une matrice génératrice de $C'^\perp$. Les lignes et les colonnes sont indexées à partir de 2 pour être cohérent avec les indices de H.

Pour $i \in [2, \ldots, s]$, on pose $\beta_i(x) = \sum_{j=2}^{s} g_{1,j}(x) h'_{i,j}(x)$.

Lemme 6 (Lemme 2.4 de [32]). *Le polynôme $g_{1,1}(x)$ divise les polynômes $\beta_i(x)$, $i \in [2, \ldots, s]$.*

On pose alors $\alpha_i(x) = \beta_i(x)/g_{1,1}(x)$.

Théorème 12 (Théorème 2.7 de [32]). *La matrice*

$$H = \left(\begin{array}{c|ccc} h_{1,1}(x) & 0 & \dots & 0 \\ \hline -\alpha_2(x) & & & \\ \vdots & & H' & \\ -\alpha_s(x) & & & \end{array}\right)$$

est une matrice génératrice du dual de C.

Ce théorème permet de construire de manière itérative une matrice du dual de C.

Chapitre 4

Image q-aire d'un $\mathcal{A}$-code

4.1 Image q-aire d'un $\mathcal{A}$-code

Dans ce chapitre, nous précisons la notion d'image q-aire dans le contexte des $\mathcal{A}$-codes et de leurs matrices génératrices.

4.1.1 Image q-aire

À tout élément $a(x)$ de $\mathcal{A}$, autrement dit, à tout polynôme de degré inférieur à m, on peut associer le m-uplet de ses coordonnées dans $\mathbb{F} = \mathbb{F}_q$.

Soit ϑ l'application qui à chaque polynômes de $\mathcal{A}$, associe son image q-aire sur $\mathbb{F}^m$, si $a(x) = \sum_{i=0}^{m-1} a_i x^i$ alors :

$$\vartheta(a(x)) = (a_0, a_1, \ldots, a_{m-1}).$$

Soit θ l'extension de ϑ à E. Autrement dit, ϑ est l'application de $E = \mathcal{A}^s$ dans $(\mathbb{F}^m)^s$, définie par :

$$\theta(e_1(x), e_2(x), \ldots, e_s(x)) = (\vartheta(e_1(x)), \vartheta(e_2(x)), \ldots, \vartheta(e_s(x)) \in \mathbb{F}^{ms}.$$

La proposition suivante donne quelques propriétés fondamentales de ϑ et θ.

Proposition 20.

- *L'application ϑ est un isomorphisme $\mathbb{F}$-linéaire de $\mathcal{A}$ sur $\mathbb{F}^m$.*
- *L'application θ est un isomorphisme $\mathbb{F}$-linéaire de $\mathcal{A}$ sur $\mathbb{F}^{ms}$.*
- *Si C est un $\mathcal{A}$-code de longueur s, alors $\theta(C)$ est un code $\mathbb{F}$-linéaire de longueur ms. De plus, $dim_{\mathbb{F}}(C) = dim(\theta(C))$.*

On note que par convention, la notation $a(x)$ sera utilisée pour désigner le polynôme $\sum_{i=0}^{m-1} a_i x^i$, et a pour designer le m-uplet $(a_0, \ldots, a_{m-1})$, en bref on a : $a = \vartheta(a(x))$.

Ainsi on peut définir l'image q-aire d'un $\mathcal{A}$-code C :

Définition 26. *Soit C un $\mathcal{A}$-code. L'image q-aire du code C est le code $\mathbb{F}$-linéaire $\mathcal{C}$ tel que : $\mathcal{C} = \theta(C)$.*

On souligne que, puisque θ est un isomorphisme, alors on peut associer à tout code $\mathcal{C}$ de longueur n sur $\mathbb{F}$ un code $C \subset E$.

En revanche, ce code C n'est pas nécessairement un $\mathcal{A}$-code, puisque ce n'est pas à priori un $\mathcal{A}$-module.

4.1.2 Image q-aire d'une base canonique de diviseurs

Dans la section 3.2.2, on a présenté une méthode systématique pour définir une matrice $\mathbb{F}$-génératrice d'un $\mathcal{A}$-code C généré par une seule ligne. Cette méthode permet d'obtenir directement une matrice génératrice de l'image q-aire. Dans ce paragraphe, nous montrons que cette méthode se généralise au cas d'un $\mathcal{A}$-code quelconque à partir de sa matrice canonique introduite au paragraphe 3.4.4.

Lemme 7. *Soit C un $\mathcal{A}$-code admettant une matrice canonique ne comportant qu'une seule ligne $g = (g_1(x), ..., g_s(x))$ (g est le générateur canonique, en particulier $g_1(x)|f(x)$). Tous les coefficients de $g_i(x)$ sont des multiples de $g_1(x)$.*

Démonstration. Soit $h(x) = f(x)/g_1(x)$. On pose $c = h(x)g \in C$. On a clairement $c_1(x) = 0$, et donc $c = 0 \times g = (0, ..., 0)$.

On en déduit que $h(x)g_i(x) = 0 \pmod{f(x)}$ pour tout i, d'où le résultat. □

L'exemple suivant présente la construction de l'image q-aire d'un tel code.

Exemple 9. *Soit $\mathbb{F} = \mathbb{F}_2$, $f(x) = (x^3 + x + 1)(x^4 + x + 1)$.*
Soit G une matrice génératrice sur $\mathcal{A}$, d'un $\mathcal{A}$-code C admettant une base canonique réduite à un élément :

$$G = \begin{pmatrix} x^3 + x + 1 & x(x^3 + x + 1) & (x^2 + 1)(x^3 + x + 1) \end{pmatrix}$$

La proposition 14, permet de calculer la matrice génératrice sur $\mathbb{F}_2$ de G :

On rappelle que $m = deg(f(x)) = 7$, et $pgcd(f(x), g_j(x)) = (x^3 + x + 1)$. Par conséquence les lignes de la matrice binaire sont obtenues en multipliant G par : x^0, x^1, x^2, et par $x^{(7-3-1)}$.

$$G' = \begin{pmatrix} x^3 + x + 1 & x(x^3 + x + 1) & (x^2 + 1)(x^3 + x + 1) \\ x^4 + x^2 + x & x^5 + x^3 + x^2 & x^6 + x^3 + x^2 + x \\ x^5 + x^3 + x^2 & x^6 + x^4 + x^3 & x^5 + x^4 + 1 \\ x^6 + x^4 + x^3 & x^4 + x^3 + x^2 + 1 & x^6 + x^5 + x \end{pmatrix}$$

alors la matrice génératrice du code image binaire de C est :

$$\mathfrak{G} = \left(\begin{array}{ccc|ccc|ccc} 1&1&0&1&0&0&0 & 0&1&1&0&1&0&0 & 1&1&1&0&0&1&0 \\ 0&1&1&0&1&0&0 & 0&0&1&1&0&1&0 & 0&1&1&1&0&0&1 \\ 0&0&1&1&0&1&0 & 0&0&0&1&1&0&1 & 1&0&0&0&1&1&0 \\ 0&0&0&1&1&0&1 & 1&0&1&1&1&0&0 & 0&1&0&0&0&1&1 \end{array}\right)$$

Soit G une matrice génératrice, constituée de la base des diviseurs d'un $\mathcal{A}$-code C, et k le nombre d'éléments de cette base.
À chaque ligne de G (ou à chaque générateur de base), on peut associer une matrice à éléments dans $\mathbb{F}$, comme dans le dernier exemple. On note par $\mathfrak{G}$ la matrice obtenue par la concaténation horizontale de ces k matrices.

Proposition 21. *Soit C un $\mathcal{A}$-code de matrice génératrice canonique G, et $\mathcal{C}$ sont image q-aire sur $\mathbb{F}$. La matrice $\mathfrak{G}$ est une matrice génératrice du code $\mathcal{C}$. En particulier $\mathfrak{G}$ est de rang plein.*

Démonstration. La proposition 14 assure que les lignes de $\mathfrak{G}$ génèrent $\mathcal{C}$, et sachant que la matrice $\mathfrak{G}$ est une matrice échelonnée, elle est alors de rang plein. □

Dans le cas des codes quasi-cycliques ($f(x) = x^m - 1$), on remarque que chaque bloc de $\mathfrak{G}$ est circulant, chose qui n'est pas toujours vraie dans le cas général (à cause de la réduction modulo $f(x)$, qui n'est pas un simple shift). Les cas des matrices $G'_{4,2}$, $G'_{3,3}$ et $G'_{4,3}$ de l'exemple 9 donnent des contre-exemples.

4.2 Dualité q-aire et $\mathcal{A}$-dualité

L'objectif de cette section est d'étudier les liens et les différences existantes entre la dualité de l'image q-aire et la dualité dans E en tant que $\mathcal{A}$-module.

4.2.1 Représentation matricielle de la multiplication

Soit $a(x)$ un élément de $\mathcal{A}$, l'application :

$$\begin{array}{rccc} \Omega_{a(x)} & : & \mathcal{A} & \longrightarrow & \mathcal{A} \\ & & u(x) & \mapsto & a(x)u(x) \end{array}$$

est une application $\mathbb{F}$-linéaire.

C'est un isomorphisme si et seulement si $pgcd(a(x), f(x)) = 1$, autrement dit, si $a(x)$ est inversible dans $\mathcal{A}$.

Puisque ϑ est un isomorphisme $\mathbb{F}$-linéaire, on peut définir l'application $\mathbb{F}$-linéaire correspondante par :

$$\Omega_a = \vartheta \; o \; \Omega_{a(x)} \; o \; \vartheta^{-1}.$$

Nous allons construire la représentation matricielle d'une telle application.

Le cas particulier $a(x) = x$ est directement lié à la matrice compagnon du polynôme $f(x)$:

$$M_x = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & 0 & 1 & 0 & \ddots & \vdots \\ \vdots & \vdots & \dots & \dots & \dots & \vdots \\ 0 & 0 & \dots & \dots & 0 & 1 \\ -f_0 & -f_1 & \dots & \dots & \dots & -f_{m-1} \end{pmatrix}$$

avec $f(x) = \sum_{i=0}^{m} f_i x^i$, et $f_m = 1$ ($f(x)$ est un polynômes unitaire).

Le lemme suivant est un résultat classique [[24]. chap.2 et [28]].

Lemme 8. *La matrice M_x est la matrice de l'application linéaire $\Omega_{\vartheta(x)}$, autrement dit :*

$$\vartheta(xe(x)) = eM_x.$$

Démonstration. On sait que $e(x) = \sum_{i=0}^{m} e_i x^i = e_0 x^0 + e_1 x^1 + \ldots + e_m x^m$, et alors $xe(x) = e_0 x + e_1 x^2 + \ldots + e_m x^{(m+1)}$.
Ainsi

$$xe(x) = \sum_{i=0}^{m} e_i x^{i+1}.$$

Puisque $f(x)$ est un polynôme unitaire alors : $f(x) = x^m + \sum_{i=0}^{m-1} f_i x^i$.
Par conséquent $x^m = -\sum_{i=0}^{m-1} f_i x^i \ mod\ f(x)$.

Il est clair que

$$xe(x) = \sum_{i=0}^{m} e_i x^{i+1} = \sum_{i=1}^{m} e_{i-1} x^i.$$

En décomposant :

$$xe(x) = \sum_{i=1}^{m-1} e_{i-1} x^i + e_m x^m = \sum_{i=1}^{m-1} e_{i-1} x^i + e_m(-\sum_{i=0}^{m-1} f_i x^i).$$

C'est pourquoi :

$$xe(x) = -e_m \sum_{i=0}^{m-1} f_i x^i + \sum_{i=1}^{m-1} e_{i-1} x^i.$$

En conséquence :

$$xe(x) = eM_x, \ \textit{pour tout polynome } e(x) \textit{ de } \mathcal{A}.$$

□

Ce résultat s'étend facilement à tout autre polynôme $a(x)$ de $\mathcal{A}$:
Si $a(x) = \sum_{i=0}^{m-1} a_i x^i$, alors $M_{a(x)} = \sum_{i=0}^{m-1} a_i M_x^i$.

À partir du lemme 8 et du fait que $\Omega_{(a(x))} = \sum_{i=0}^{m-1} a_i \Omega_x^i$, on peut en déduire la proposition suivante :

Proposition 22.
La matrice $M_{a(x)}$ est la matrice de l'application linéaire $\Omega_{\vartheta(a(x)}$:

$$\vartheta(a(x)u(x)) = uM_{a(x)}.$$

4.2.2 Matrice q-aire associée à la structure de $\mathcal{A}$-module

On commence par introduire une autre notion de "matrice génératrice " (qui ne sera pas nécessairement de rang plein) pour l'image q-aire d'un $\mathcal{A}$-code qui prend en compte la structure sous-jacente de $\mathcal{A}$-module. Cette approche simplifiera la construction du $\mathcal{A}$-dual d'un $\mathcal{A}$-code.

Soit $G = (g_{i,j}(x))$ une matrice de taille $k \times s$ sur $\mathcal{A}$, on pose

$$\Gamma(G) = \begin{pmatrix} M_{g_{1,1}(x)} & M_{g_{1,2}(x)} & \dots & M_{g_{1,s}(x)} \\ \vdots & \vdots & \vdots & \vdots \\ M_{g_{k,1}(x)} & M_{g_{k,2}(x)} & \dots & M_{g_{k,s}(x)} \end{pmatrix}$$

Théorème 13. *Soit G une matrice génératrice d'un $\mathcal{A}$-code C, de longueur s sur $\mathcal{A}$. Les lignes de la matrice $\Gamma(G)$, génèrent $\mathcal{C} = \theta(C)$. La matrice $\Gamma(G)$ n'est à priori pas de rang plein.*

Démonstration. Soient $g^{(i)}$ les lignes de G, pour $1 \leq i \leq k$. Soit $c = \sum_{i=1}^{k} h_i(x) g^{(i)}$ un élément de C.

On pose $u = \theta(h_1(x), \dots, h_s(x)) \in \mathbb{F}^{ms}$. On déduit de la proposition 22 que $\theta(c) = u\Gamma(G)$.

Réciproquement, si $s = u\Gamma(G)$ et $(h_1(x), \dots, h_s(x)) = \theta^{-1}(u)$, alors on a

$$\theta^{-1}(s) = (h_1(x), \dots, h_s(x))G \in C$$

. □

4.2.3 Construction du dual d'un $\mathcal{A}$-code

À partir d'une matrice $G = (g_{i,j}(x))$ de taille $k \times s$ sur $\mathcal{A}$, on peut construire une autre matrice de taille $(km) \times (sm)$ sur $\mathbb{F}$ en remplaçant chaque entrée de G par la matrice transposée de la matrice $M_{g_{i,j}(x)}$ de taille $m \times m$:

$$\Upsilon(G) = \begin{pmatrix} M^t_{g_{1,1}(x)} & M^t_{g_{1,2}(x)} & \dots & M^t_{g_{1,s}(x)} \\ \vdots & \vdots & \vdots & \vdots \\ M^t_{g_{k,1}(x)} & M^t_{g_{k,2}(x)} & \dots & M^t_{g_{k,s}(x)} \end{pmatrix}$$

Le résultat principal de ce paragraphe est que cette matrice permet d'introduire un lien entre la $\mathcal{A}$-dualité dans $E = \mathcal{A}^s$ et la $\mathbb{F}$-dualité sur $\mathbb{F}^{ms}$.

Théorème 14. *Si G est une matrice génératrice d'un $\mathcal{A}$-code C, alors la matrice $\Upsilon(G)$ génère le code $\mathbb{F}$-dual de $\theta(C^{\perp})$.*

Démonstration. On remarque que les deux matrices $\Gamma(G)$ et $\Upsilon(G)$ ont le même rang (même si leur rang n'est pas plein). Ainsi à partir des lignes de $\Upsilon(G)$, on peut obtenir un système de générateurs pour le code. Mais $\Upsilon(G)$ n'est pas une matrice génératrice au vrai sens du terme.

Un élément $h \in E$ est aussi un élément de $C^{\perp}$, si et seulement si pour $i = 1$ à k, $< h, g^{(i)} > = \sum_{j=1}^{l} h_j(x) g_{i,j}(x) = 0$.
En appliquant la proposition 22, on obtient :

$$\theta\Big(\sum_{j=1}^{s} h_j(x) g_{i,j}(x)\Big) = \sum_{j=1}^{s} \theta(h_j(x)) M_{g_{i,j}(x)} = 0.$$

Par transposition, on déduit que :

$$\sum_{j=1}^{s} M^t_{g_{i,j}(x)} \theta(h_j(x))^t = 0$$

ou autrement

$$(M^t_{g_{i,1}(x)}, \ldots, M^t_{g_{i,s}(x)}) \theta(h)^t, \ \textit{pour } i = 1, \ldots, k.$$

Ce qui est équivalent à dire que :

$$\Upsilon(G) \theta(h)^t = 0, \ \textit{pour tout } h \textit{ dans } C^{\perp}.$$

□

4.2.4 Lien entre $\mathcal{A}$-dualité et dualité q-aire

Cas des codes cycliques

On s'intéresse ici au cas particulier $s = 1$ et $f(x) = x^m - 1$.

Si $a(x)$ est un polynôme de $\mathcal{A}$, on pose $\overline{a(x)} = \sum_{i=0}^{d} a_i x^{m-1-i}$. On peut remarquer que, si $d = deg(a(x))$, alors $\overline{a(x)}$ est presque le polynôme réciproque de $a(x)$. En effet, on a $\overline{a(x)} = x^{m-d} rec(a(x))$.

Si $g(x) | (x^m - 1)$ est un polynômes générateur du code cyclique C sur $\mathcal{A}$, alors son $\mathcal{A}$-dual est généré par $h(x) = (x^m - 1)/g(x)$. Il est bien connu que le dual de son image q-aire est le code cyclique engendré par le polynôme réciproque $rec(h(x))$. Le dual q-aire est donc aussi engendré par le polynôme $\overline{h(x)}$.

Le lemme suivant nous permet de faire le lien entre le $\mathcal{A}$-dual et le dual q-aire.

Lemme 9. *Soit $a(x)$ un élément de $\mathcal{A}$, sous l'hypothèse $f(x) = x^m - 1$, on a la relation suivante :*

$$M^T_{a(x)} = M_{\overline{a(x)}}.$$

Démonstration. Ce résultat découle directement de la propriété :

$$M_{x^{m-1}} = M^T_x.$$

□

En utilisant le théorème 14 et le lemme 9, on a la proposition suivante :

Proposition 23. *Soit C un $\mathcal{A}$-code cyclique (c'est-à-dire $s = 1$ et $f(x) = x^m - 1$). Les codes $\theta(C^{\perp})$ et $\theta(C)^{\perp}$ sont équivalents par la permutation des indices $i \mapsto m - 1 - i$.*

Cas des codes quasi-cycliques

La généralisation de la propriété précédente sur les codes cycliques au cas des codes quasi-cycliques est donnée dans [23]. En particulier si $s \geq 1$ et $f(x) = x^m - 1$, l'image q-aire du code quasi-cyclique est équivalente par permutation au code $\mathbb{F}$-dual de l'image q-aire de son $\mathcal{A}$-dual.

Par contre ce résultat ne se généralise pas à $f(x)$ (même dans le cas où $f(x)$ n'a pas de racine multiple). Par conséquent le $\mathbb{F}$-dual de l'image q-aire d'un $\mathcal{A}$-code, n'est pas toujours l'image q-aire d'un autre $\mathcal{A}$-code C'.

Exemple 10. *On considère le $\mathcal{A}$-code introduit dans l'exemple 3, son image binaire est le code binaire de paramètres* $[21, 11, 3]$*, le code $\mathbb{F}$-dual de l'image binaire du code $\mathcal{A}$-dual $C^{\perp}$ est le code binaire de paramètres* $[21, 11, 2]$*. Ainsi ces deux codes ne peuvent pas être équivalents.*

De plus, le code $\mathbb{F}$-dual $C^{\perp_{\mathbb{F}}}$ de l'image q-aire de C, est différent de l'image q-aire d'un certain $\mathcal{A}$-code. Autrement dit, $\theta^{-1}(\mathcal{C}^{\perp_{\mathbb{F}}})$ est un $\mathbb{F}$-sous espace vectoriel de E, en revanche il n'est pas un $\mathcal{A}$-sous module de E.

Troisième partie

Codes additifs sur $\mathbb{F}_2^m$

Partie III : Codes additifs sur $\mathbb{F}_2^m$

Introduction :

Après avoir étudié les codes sur une structure d'anneaux quotient dans la deuxième partie de cette thèse, dans cette partie, et pour des raisons d'optimisation des applications cryptographiques, on ôte un peu de la structure, en particulier, nous présentons une étude des codes sur le groupe additif $\mathcal{F} = (\mathbb{F}_2^m, +)$, les mots de ces codes sont des s-uplets de m-uplets binaires car on s'intéresse aux propriétés entre les blocs, plutôt qu'aux propriétés binaires. Notre étude se polarise sur les codes additifs systématiques, que nous appelons des $\mathcal{F}$-codes. Nous définissons leur matrice génératrice systématique. L'image binaire de ces codes nous permet de mettre en évidence le lien entre un code linéaire sur le corps fini $\mathbb{F}_{2^m}$ et un code additif sur $(\mathbb{F}_2^m, +)$. Nous nous intéressons à la notion de codes MDS additifs, et nous définissons une isométrie pour l'équivalence des $\mathcal{F}$-codes. L'inspection des structures d'anneau possibles sur $\mathbb{F}_2^m$, nous permet d'identifier celles sur lesquelles il est intéressant de construire des matrices MDS pour la diffusion.

Les coefficients de la matrice génératrice des $\mathcal{F}$-codes étant des éléments de l'anneau $\mathcal{L}$ des endomorphisme de $\mathbb{F}_2^m$, alors nous avons considéré les codes définis sur cet anneau d'endomorphismes. Dans ce contexte un code linéaire est un $\mathcal{L}$-sous-module à gauche. Nous appelons ces codes linéaires sur $\mathcal{L}$ des $\mathcal{L}$-codes. Nous étudions la notion de dualité dans ce contexte, et le lien avec leur image binaire et la dualité de l'image binaire. Nous terminons cette partie par une étude des codes linéaires sur certains sous anneaux de $\mathcal{L}$, la finalité étant la recherche de codes MDS.

L'objectif global de cette partie est d'étudier les structures sur lesquelles il sera intéressant de construire des matrices MDS de diffusion pour la cryptographie. Ce point sera détaillé au chapitre suivant. Les résultats de cette partie on fait l'objet de la publication [9].

La liste des principaux symboles utilisés dans la partie III :

— $\mathcal{F} = (\mathbb{F}_2^m, +)$: le groupe additif abélien de $\mathbb{F}_2^m$.
— $\mathcal{L}$: l'anneau des $\mathbb{F}_2$-endomorphismes de $\mathcal{F}$ dans $\mathcal{F}$.
— $E = \mathcal{F}^s$ ou $\mathcal{L}^s$ suivant le contexte.
— $\mathcal{F}$-code : un code additif sur $\mathcal{F}$.
— $\mathcal{L}$-code : un sous-modules à gauche de $\mathcal{L}^s$.
— $\mathcal{C}$: un $\mathcal{F}$-code.
— $\mathcal{C}$: un $\mathcal{L}$-code.
— s : la longueur des $\mathcal{F}$-codes et des $\mathcal{L}$-codes.
— k : la pseudo dimension d'un $\mathcal{F}$-code ou d'un $\mathcal{L}$-code.
— $n = ms$: la longueur de l'image binaire d'un $\mathcal{F}$-code ou d'un $\mathcal{L}$-code.
— mk : la dimension de l'image binaire d'un $\mathcal{F}$-code ou d'un $\mathcal{L}$-code.
— $\mathcal{M}$: une matrice à coefficients dans $\mathcal{L}$.
— M_ϕ : la matrice binaire de $\phi \in \mathcal{L}$, de taille $m \times m$, relative à la base canonique de $\mathbb{F}_2^m$.
— $GL(m, 2)$: le groupe linéaire des matrices inversibles de taille $m \times m$, à coefficients dans $\mathbb{F}_2$.
— $Mon_{\mathcal{L}}$: le groupe des matrices monomiales de taille $s \times s$ à coefficients dans $\mathcal{L}$, admettant un et un seul coefficient non-nul par ligne et par colonne, ce coefficient étant dans $GL(m, 2)$.
— $\mathcal{R}$: l'anneau $(\mathcal{F}, +, *)$, avec $(\mathcal{F}, +)$ est le groupe abélien pour l'addition coordonnée par coordonnée et $*$ est la multiplication de Hadamard.
— $\mathcal{R}$-code : un $\mathcal{F}$-code $\mathcal{R}$-linéaire (sous-module de $\mathcal{R}^s$).
— K_i : le corps $\mathbb{F}(x)/f_i(x)$, avec $f_i(x)$ un polynôme irréductible.
— M_ϕ^T : la matrice transposée de la matrice binaire de ϕ.
— ϕ^T : un endomorphisme de $\mathcal{L}$, dont la matrice binaire associée est M_ϕ^T.
— $\mathcal{C}^\perp$: le code dual d'un $\mathcal{L}$-code $\mathcal{C}$.
— C : l'image binaire d'un $\mathcal{F}$-code $\mathcal{C}$.
— $\mathcal{C}^{\perp *}$: le code dual binaire du $\mathcal{L}$-code $\mathcal{C}$.
— $< \varphi, \psi >_T = \sum_{i=1}^{s} \varphi_i \psi_i^T$, avec $\varphi, \psi \in \mathcal{L}^s$.
— $\mathcal{M}^* = (\alpha_{i,j}^T)$: la matrice transposée des endomorphismes dont la matrice binaire associe est $M = (\alpha_{i,j})$.
— $\varphi^* = (\varphi_1^T, \ldots, \varphi_s^T)$.

Chapitre 5

Codes additifs sur $\mathbb{F}_2^m$

Ce chapitre s'intéresse aux codes additifs dont l'alphabet est $(\mathbb{F}_2^m, +)$. Les propriétés de ces codes sont très proches de celles des codes binaires, puisqu'ils sont en particulier $\mathbb{F}_2$-linéaires, mais nous nous intéressons aux propriétés des blocs de m bits dans la perspective de la cryptographie symétrique.

Pour des raisons d'optimisation des implémentations machines des applications cryptographiques, il est important d'utiliser des opérations simples comme le XOR, d'où notre choix du groupe additif. La taille classique des blocs sera $m = 4$, 8 et parfois 16, ces tailles correspondent aux tailles des Sboxes utilisées en cryptographie.

5.1 Codes m-bloc additifs sur $(\mathbb{F}_2^m, +)$

5.1.1 Codes sur un groupe fini

On considère dans ce paragraphe les codes de longueur s définis sur un alphabet fini $\mathcal{F}$ muni d'une structure de groupe additif abélien $(\mathcal{F}, +)$. Dans ce cas $E = \mathcal{F}^s$ est lui-même un groupe additif. Cela conduit naturellement à définir les codes sur un groupe.

Définition 27. *Soient $(\mathcal{F}, +)$ un groupe commutatif et $E = \mathcal{F}^s$. Un code additif $\mathcal{C}$ de longueur s sur $\mathcal{F}$ est un sous-groupe de $(E, +)$.*

Un des intérêts des codes additifs sur un groupe fini est le fait qu'il suffit de connaître un système de générateurs additifs d'un code pour le décrire et éventuellement l'encoder.

On peut remarquer que, pour un code additif $\mathcal{C}$, la distance minimale du code est simplement le poids minimal des mots de codes non nuls, puisqu'on peut toujours se ramener à la distance entre un mot de code et le s-uplet nul par translation.

Il existe de nombreux travaux sur ce type de codes. Dans cette thèse, nous nous intéressons uniquement au cas particulier $\mathcal{F} = (\mathbb{F}_2^m, +)$ qui modélise les blocs de bits utilisés en cryptographie symétrique.

5.1.2 $\mathcal{F}$-codes additifs

Dans la suite de ce document $\mathcal{F}$ désigne le groupe additif $(\mathbb{F}_2^m, +)$.

Définition 28. *Un code m-bloc additif (binaire) de longueur s est un code additif sur $\mathcal{F}$ de longueur s.*

Dans la suite on appelle un tel code un $\mathcal{F}$-code ou simplement un code additif lorsqu'il n'y aura pas d'ambiguïté.

Dans le cas d'un code m-bloc additif, on ne peut pas multiplier par un scalaire de $\mathbb{F}_2^m$. Conséquemment c'est un $\mathbb{F}_2$ sous espace vectoriel de $\mathbb{F}_2^{m\times s}$.

Exemple 11. *le code* $\{((0111),(1100));((0100),(0101));((0001),(0010))\}$ *est un code 4-bloc additif de longueur* 2 *sur* $\mathbb{F}_2^4$.

En tirant profit de l'isomorphisme de groupe $E \simeq \mathcal{F}^s \simeq \mathbb{F}_2^{ms}$, un code m-bloc $\mathcal{C}$ de longueur s est aussi un code linéaire binaire de longueur $n = sm$ sur $\mathbb{F}_2$. Un mot c de $\mathcal{C}$ est un s-uplet de m-uplets binaires $c = (c_1, \ldots, c_s)$ tel que $c_i = (c_{i,1}, \ldots, c_{i,m}) \in \mathbb{F}_2^m$ pour $i \in [1, \ldots, s]$.

Toutefois dans cette thèse on s'intéresse aux propriétés entre les m-blocs plutôt qu'aux propriétés binaires. Plus précisément, on ne regarde pas à l'intérieur des blocs, mais on considère chaque bloc comme étant un élément, et on étudie les relations entre ces éléments. Par exemple le poids de Hamming d'un mot de $\mathcal{C}$ est le poids en bloc de ce mot.

En vue des applications et pour simplifier les résultats, nous limitons notre étude à un type spécial de codes m-bloc additifs qui est celui des codes m-bloc additifs systématiques.

5.2 Codes additifs systématiques

5.2.1 Encodage systématique

Un code est dit systématique au sens strict si les k premières positions des mots du code sont exactement les k symboles du message à encoder. On peut remarquer que, si q est la taille de l'alphabet, alors le code a exactement q^k éléments.

Il est dit systématique au sens large s'il existe un ensemble de k positions tel que, pour tout mot du code, les k symboles correspondants sont ceux du message à encoder. Un code systématique au sens large est équivalent par permutation des symboles à un code systématique au sens strict.

Il est à noter que tout code linéaire C de longueur n et de dimension k, est un code systématique au sens large. En effet, si G est une matrice génératrice de C, elle est de rang k, il existe donc k colonnes de G linéairement indépendantes. Par permutation, on peut ramener ces colonnes sur les k premières positions. Il suffit alors d'appliquer une élimination Gaussienne pour obtenir une matrice génératrice sous la forme $(I_k \mid B_{n-k})$. En fait la notion de code systématique est en relation étroite avec la notion de fonction d'encodage systématique.

Définition 29. *Une fonction d'encodage systématique (au sens strict)* $\Phi : \mathcal{F}^k \mapsto E = \mathcal{F}^s$ *est une application* $\mathbb{F}_2$*-linéaire telle que, pour tout élément* $x \in \mathcal{F}^k$*, on ait :*

$$\Phi(x) = (x_1, \ldots, x_k, \phi_1(x), ..., \phi_r(x))$$

avec $r = s - k$ *(redondance) et les fonctions* ϕ_i *sont des fonctions* $\mathbb{F}_2$*-linéaires de* $\mathcal{F}^k$ *dans* $\mathcal{F}$*.*

5.2.2 Matrice génératrice d'un $\mathcal{F}$-code systématique

Soit $\mathcal{C}$ un code additif systématique de longueur s sur $\mathcal{F}$, et Φ sa fonction d'encodage définie au paragraphe précédent.

On note $\mathcal{L}$ l'anneau des $\mathbb{F}_2$-endomorphismes de $\mathcal{F}$ dans $\mathcal{F}$.

Les r applications linéaires ϕ_i qui définissent Φ peuvent elles-même se décomposer en une somme de k éléments de $\mathcal{L}$: $\phi_i(x) = \sum_{j=1}^{k} \varphi_{i,j}(x_j)$ pour $\varphi_{i,j}$ dans $\mathcal{L}$ et $1 \leq i \leq k$.

En utilisant cette décomposition on est capable de construire une "matrice génératrice systématique" $\mathcal{G}$ du code $\mathcal{C}$:

$$\mathcal{G} = \begin{pmatrix} Id & 0 & \cdots & \cdots & 0 & \varphi_{1,1} & \varphi_{1,2} & \cdots & \varphi_{1,r} \\ 0 & Id & \cdots & \cdots & 0 & \varphi_{2,1} & \varphi_{2,2} & \cdots & \varphi_{2,r} \\ \vdots & \ddots & \ddots & \ldots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & Id & \varphi_{k,1} & \varphi_{k,2} & \cdots & \varphi_{k,r} \end{pmatrix}$$

Un mot c du code $\mathcal{C}$ est alors $c = x.\mathcal{G}$, avec $x = (x_1, x_2, \ldots, x_k)$ dans $\mathcal{F}^k$.

Par convention et cohérence avec les notations matricielles, on a, pour tout a de $\mathcal{F}$ et ϕ de $\mathcal{L}$, $a\phi = \phi(a)$. De même, pour ϕ et ψ de $\mathcal{L}$, on pose $\phi\psi = \psi \circ \phi$.

Cette approche de construction de matrice génératrice peut se généraliser directement aux codes systématiques au sens large et aux matrices génératrices non obligatoirement systématiques de $\mathcal{F}$-codes systématiques. La restriction aux codes systématiques assure que la $\mathbb{F}_2$-dimension du $\mathcal{F}$-code est bien km. Cette approche sera développée au chapitre 6.

5.3 Image binaire d'un $\mathcal{F}$-code

5.3.1 Image binaire d'un code additif

Comme nous l'avons fait au chapitre 4.1 pour l'image q-aire d'un $\mathcal{A}$-code, on peut naturellement définir l'image binaire d'un $\mathcal{F}$-code. Pour cela, il suffit d'utiliser le $\mathbb{F}_2$-isomorphisme $E \simeq \mathbb{F}_2^{ms}$.

On peut directement tirer profit de la matrice de l'encodage systématique Φ pour obtenir la matrice génératrice systématique de l'image binaire.

À chaque endomorphisme linéaire φ de $\mathcal{L}$, on associe sa matrice binaire M_φ de taille $m \times m$ sur la base canonique de $\mathbb{F}_2^m$: pour tout $u = (u_1, \ldots, u_m) \in \mathbb{F}_2^m$, si $v = \varphi(u) \in \mathbb{F}_2^m$, alors $v = uM_\varphi$.

L'image binaire de la matrice génératrice systématique $\mathcal{G}$ définie ci-dessus est :

$$G_b = \begin{pmatrix} I_m & 0_m & \cdots & 0_m & M_{\varphi_{1,1}} & \cdots & M_{\varphi_{1,r}} \\ 0_m & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0_m & \vdots & & \vdots \\ 0_m & \cdots & 0_m & I_m & M_{\varphi_{k,1}} & \cdots & M_{\varphi_{k,r}} \end{pmatrix}$$

telle que $M_{\varphi_{i,j}}$ est la matrice binaire de l'endomorphisme $\varphi_{i,j}$, avec la convention $\Phi(x) = x.\mathcal{M}$ et $\mathcal{M} = (M_{\varphi_{i,j}})$, pour $1 \leq i \leq k$ et $1 \leq j \leq r$.

À tout $\mathcal{F}$-code systématique de pseudo-dimension k, on peut associer un code binaire C de longueur $n = ms$ et dimension mk. Et naturellement, à tout code binaire C systématique de longueur $n = ms$ on peut associer un $\mathcal{F}$-code systématique de longueur s. Mais cela n'est pas vrais dans le cas d'un code binaire non systématique.

Exemple 12. *Pour $m = 3$, $s = 3$ et $k = 5$ Soit G une matrice génératrice d'un code binaire non systématique :*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

La permutation des colonnes donne :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

On pause $M_{\varphi_{1,1}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $M_{\varphi_{1,2}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $M_{\varphi_{1,3}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$,

$M_{\varphi_{2,1}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $M_{\varphi_{2,2}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $M_{\varphi_{1,3}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

La matrice $\mathcal{G} = (\varphi_{i,j})$, pour $i \in [1;2]$ et $j \in [1;3]$ des endomorphismes correspondants aux matrices binaires ci-dessus est une matrice génératrice non systématique d'un $\mathcal{F}$-code.

5.3.2 Lien entre les codes linéaires sur $\mathbb{F}_{2^m}$ et $\mathcal{F}$-codes

L'image binaire d'un code linéaire sur $\mathbb{F}_{2^m}$ a fait l'objet de nombreuses études. Cette identification se fait en choisissant une base de $\mathbb{F}_{2^m}$ sur $\mathbb{F}_2$ et en

remplaçant chaque élément a du corps $\mathbb{F}_{2^m}$ par ses coordonnées binaires.

En fait cette identification conduit naturellement à regarder l'image d'un tel code en tant que $\mathcal{F}$-code. En particulier la notion de distance de Hamming sur $\mathbb{F}_{2^m}$ coïncide avec la distance par bloc des $\mathcal{F}$-codes.

Il est facile de vérifier que, si un $\mathcal{F}$-code est l'image d'un code linéaire sur $\mathbb{F}_{2^m}$, alors ce $\mathcal{F}$-code est systématique.

En suivant l'approche de la section 5.3.1, à partir de la matrice génératrice systématique d'un code de paramètres $[s, k]$ sur $\mathbb{F}_{2^m}$, on peut construire la matrice d'encodage systématique du $\mathcal{F}$-code correspondant décrite dans la section 5.2.2.

Soit a un élément de $\mathbb{F}_{2^m}$. La multiplication par a dans $\mathbb{F}_{2^m}$ est une application $\mathbb{F}_2$-linéaire que l'on note φ_a. Lorsqu'on a fixé une base pour identifier l'espace vectoriel $\mathbb{F}_{2^m}$ à $\mathbb{F}_2^m$, on obtient une matrice $m \times m$ binaire M_{φ_a} associée à l'application linéaire φ_a.

Si G est une matrice génératrice d'un code linéaire sur $\mathbb{F}_{2^m}$, on obtient sa matrice d'encodage systématique $\mathcal{G}$ en remplaçant les entrées $\alpha_{i,j}$ de G par $\varphi_{\alpha_{i,j}}$.

De même, on obtient la matrice systématique de l'image binaire G_b en remplaçant les entrées $\alpha_{i,j}$ de G par les matrices $M_{\varphi_{\alpha_{i,j}}}$.

5.4 Codes additifs MDS

Conformément à la définition 12, un $\mathcal{F}$-code est MDS (par bloc) s'il vérifie l'égalité $\#\mathcal{C} = (2^m)^{s-d+1}$.

On remarque que, si un $\mathcal{F}$-code $\mathcal{C}$ est MDS, alors il existe un entier k tel que $\#\mathcal{C} = 2^{mk}$. Comme précédemment, on appelle k sa pseudo-dimension, puisqu'on a $\#\mathcal{C} = q^k$, avec $q = 2^m$ qui est la taille de l'alphabet $\mathcal{F}$.

Définition 30. *Un ensemble d'information d'un code additif $\mathcal{C}$ de pseudo-dimension k est un sous-ensemble I d'un support de taille k, tel que $p_I(\mathcal{C}) = \mathcal{F}^k$, où p_I est la projection de $\mathcal{F}^s$ sur $\mathcal{F}^k$ qui ne conserve que les coordonnées d'indices dans I.*

Si I est un ensemble d'information, alors p_I est une bijection de $\mathcal{C}$ sur $\mathcal{F}^k$.

La proposition suivante est une généralisation du [[26], Ch.11, corollaire 3].

Proposition 24. *Un code additif $\mathcal{C}$ est MDS si et seulement si tout sous-ensemble I du support de taille k est un ensemble d'information pour $\mathcal{C}$.*

Démonstration. s'il existe un ensemble de k coordonnées, et qui n'est pas un ensemble d'information, alors il existe un mot de code non nul qui s'annule sur ces k positions, et réciproquement. Dans les deux cas, la distance minimale du code est strictement inférieure à $n - k + 1$. □

Il résulte en particulier de cette proposition, que tout code additif MDS $\mathcal{C}$ a une matrice génératrice sous forme systématique stricte. Il est donc un code additif systématique au sens strict.

Le théorème suivant est une généralisation du [[26], chap.11, théorème 8].

Théorème 15. *Soit $\mathcal{C}$ un code additif systématique, et $\mathcal{G} = (\mathcal{I}_k|\mathcal{M}_{k\times r})$ sa matrice génératrice systématique (à coefficients dans $\mathcal{L}$). Le code $\mathcal{C}$ est MDS si et seulement si chaque sous-matrice carrée (formée par i lignes et i colonnes, avec $i \in [1; min(k, s-k)]$) de m-bloc est la matrice d'un automorphisme de E^i (c'est-à-dire elle est inversible).*

Démonstration. La démonstration est la même que celle donnée dans [26]. La seule différence est que, si on considère une matrice d'endomorphismes, les coefficients ne sont pas forcément commutatifs, la notion de déterminant non nul est remplacée par la notion de matrice inversible. □

En fait, lorsqu'on passe à l'image binaire de la matrice, on retombe à nouveau sur une notion de déterminants binaires.

L'application à la cryptographie de notre approche sera présentée dans la dernière partie de cette thèse. On peut cependant déjà mentionner que la plupart des travaux faits sur les matrices MDS pour la cryptographie (par exemple dans [[2], [37], [47]]) sont effectués avec des matrices où les coefficients commutent entre eux, et donc pour lesquelles la notion de déterminant existe.

5.5 Équivalence des $\mathcal{F}$-codes

L'objectif de ce paragraphe est d'étendre aux codes additifs les résultats sur l'équivalence des codes linéaires rappelés à la section 2.3.5.

Deux codes C et C' linéaires sur un corps $\mathbb{F}_q$ sont équivalents s'il existe une isométrie θ, $\mathbb{F}_q$-linéaire de $\mathbb{F}_q^s$ telle que $\theta(C) = C'$. D'autre part, les isométries pour la distance de Hamming sont connues [11]. Il s'agit des éléments du groupe engendré par les permutations du support et les multiplications par des scalaires non nuls sur chaque composante. D'un point de vue matriciel, il s'agit du groupe des matrices $s \times s$ monomiales qui ont un et un seul coefficient non nul par ligne et par colonne. MacWilliams dans sa thèse de doctorat [27] a montré que sur les corps finis, toute isométrie de Hamming entre des codes linéaires peut être étendue à une transformation monomiale.

On définit d'abord le groupe des matrices monomiales $Mon_{\mathcal{L}}$ comme étant le groupe des matrices de taille $s \times s$ à coefficients dans $\mathcal{L}$ admettant un et un seul coefficient non nul par ligne et par colonne, ce coefficient devant en plus appartenir au groupe linéaire $GL(m, 2)$ (c'est-à-dire être inversible). Ce groupe est engendré par les permutations des coordonnées et les matrices diagonales inversibles (les éléments de la diagonale sont dans $GL(2, m)$).

La proposition suivante énonce le fait qu'il n'y a pas d'autres $\mathcal{F}$-isométries que celles engendrées par ces deux types de transformation.

Proposition 25. *Le groupe des $\mathcal{F}$-isométries de $E = \mathcal{F}^s$ est le groupe monomial $Mon_{\mathcal{L}}$.*

Démonstration. On vérifie de manière évidente que les permutations des coordonnées et les multiplications des coordonnées par des éléments du groupe

linéaire sont des $\mathcal{F}$-isométries de E. Le groupe des matrices monomiales $Mon_{\mathcal{L}}$ est donc contenu dans le groupe des isométries de E.

Réciproquement si on regarde les images des éléments de poids 1 par une isométrie de E, les positions des coefficients non nuls de l'image déterminent entièrement la permutation sous-jacente. La valeur de chaque scalaire définit quant à elle entièrement une $\mathbb{F}_2$-isométrie de $\mathcal{F}$, c'est-à-dire le "scalaire" dans $GL(m, 2)$ correspondant à cette position. □

On peut maintenant définir l'équivalence entre deux codes additifs de longueur s sur $\mathcal{F}$ de la manière suivante :

Définition 31. *Deux $\mathcal{F}$-codes $\mathcal{C}$ et C' sont équivalents s'il existe une matrice monomiale $\mathcal{M} \in Mon_{\mathcal{L}}$ telle que $\mathcal{C}' = \mathcal{C}\mathcal{M}$.*

5.6 Structures d'anneau sur $\mathbb{F}_2^m$

Dans cette section, nous explorons les principaux anneaux dont le groupe additif est l'ensemble des m-uplets binaires muni de l'addition coordonnée par coordonnée $(\mathcal{F}, +)$.

Chaque structure d'anneau permet de définir les codes linéaires associés, c'est-à-dire les sous modules du module E correspondant. Nous allons voir que nous retrouvons des résultats classiques, mais ceux-ci peuvent cependant être très utiles dans la construction de certaines matrices MDS pour la cryptographie comme nous le verrons dans la dernière partie de cette thèse.

5.6.1 Codes sur $(\mathbb{F}_2^m, +, *)$

La structure d'anneau la plus simple sur $\mathcal{F}$ est construite à partir de la multiplication de Hadamard, c'est-à-dire la multiplication coordonnée par coordonnée. On note $\mathcal{R} = (\mathcal{F}, +, *)$ l'ensemble $\mathcal{F}$ muni de cette structure de module.

Muni de cette multiplication, $\mathcal{R}$ est en fait isomorphe au produit de corps $\mathbb{F}_2 \times \mathbb{F}_2 ... \times \mathbb{F}_2$. Ce module est commutatif. On peut en déduire facilement la structure de ses idéaux.

Pour $i \in [1; m]$, on note par e_i l'élément de $\mathcal{R}$ tel que $e_{i,i} = 1$ et $e_{i,j} = 0$ pour $i \neq j$, et par π_i la projection des éléments de $\mathcal{R}$ tel que $\pi_i(x) = \pi_i(x_1, \ldots, x_m) \mapsto x_i$.

Les idéaux minimaux de $\mathcal{R}$ sont les idéaux engendrés par les éléments e_i, et les projections p_i sont en fait les projections canoniques sur les différents corps de l'isomorphisme. Les idéaux de $\mathcal{R}$ sont alors la somme des idéaux minimaux qu'ils contiennent.

L'ensemble $E = \mathcal{F}^s$ hérite naturellement de la structure du module $\mathcal{R}$, la multiplication dans E est également le produit de Hadamard, que l'on peut voir au niveau des bits ou des blocs de bits.

Définition 32. *Un $\mathcal{F}$-code $\mathcal{C}$ est $\mathcal{R}$-linéaire si c'est un sous-module de $E = \mathcal{R}^s$. On dira que $\mathcal{C}$ est un $\mathcal{R}$-code.*

Soit $\mathcal{C}$ un $\mathcal{F}$-code. À partir de $\mathcal{C}$, on peut construire différents codes dérivés de $\mathcal{C}$: pour $i \in [1; m]$, on pose

$$e_i\mathcal{C} = \{e_i c = (e_i * c_1, \ldots, e_i * c_s) | c \in \mathcal{C}\} \subset \mathcal{R}^s$$

et

$$\pi_i(\mathcal{C}) = \{\pi_i(c) = (\pi_i(c_1), \ldots, \pi_i(c_s)) | c \in \mathcal{C}\} \subset \mathbb{F}_2^s.$$

Le résultat suivant caractérise entièrement les $\mathcal{R}$-codes.

Proposition 26. *Un $\mathcal{F}$-code est $\mathcal{R}$-linéaire (i.e. est un $\mathcal{R}$-code) si et seulement s'il est la somme directe des codes $e_i\mathcal{C}$, pour $i \in [0; m-1]$. Dans ce cas il est isomorphe à la somme directe des codes $\pi_i(\mathcal{C})$.*

Démonstration. Si $\mathcal{C}$ est un $\mathcal{R}$-module, alors $e_i * c$ appartient à $\mathcal{C}$ pour tout i, $1 \leq i \leq m$ et tout $c \in \mathcal{C}$. Les codes $e_i\mathcal{C}$ sont donc des sous-codes de $\mathcal{C}$. Pour tout élément $c \in E$, on a $c = \sum_{i=1}^{m} e_i * c$. De plus, $e_i\mathcal{C} \cap e_j\mathcal{C} = \{0\}$, pour $i \neq j$. Donc $\mathcal{C}$ est la somme directe des $e_i\mathcal{C}$. Il est immédiat de vérifier que la somme directe des e_iC est un $\mathcal{R}$-module.

La dernière propriété provient de l'isomorphisme entre $e_i\mathcal{C}$ et $\pi_i(\mathcal{C})$. En effet, par construction, les coefficients binaires des coordonnées des mots du code $e_i\mathcal{C}$ sont tous nuls excepté éventuellement la i-ème coordonnée.

□

Le corollaire suivant donne la relation entre la distance minimale d'un code linéaire et ses projections :

Corollaire 1. *La distance minimale d'un $\mathcal{R}$-code $\mathcal{C} \neq \{0\}$ est le minimum des distances minimales de ses codes projections binaires non nuls $\pi_i(\mathcal{C})$.*

Exemple 13. *On pose $m = 3$, $k = 2$ et $s = 5$. On considère le $\mathcal{F}$-code $\mathcal{C}$ dont l'image binaire de la $\mathcal{L}$-matrice génératrice systématique est :*

$$G = \left(\begin{array}{ccccc} 1\,0\,0 & 0\,0\,0 & 0\,0\,0 & 1\,0\,0 & 1\,0\,0 \\ 0\,1\,0 & 0\,0\,0 & 0\,1\,0 & 0\,0\,0 & 0\,1\,0 \\ 0\,0\,1 & 0\,0\,0 & 0\,0\,1 & 0\,0\,0 & 0\,0\,0 \\ \hline 0\,0\,0 & 1\,0\,0 & 1\,0\,0 & 0\,0\,0 & 1\,0\,0 \\ 0\,0\,0 & 0\,1\,0 & 0\,1\,0 & 0\,1\,0 & 0\,1\,0 \\ 0\,0\,0 & 0\,0\,1 & 0\,0\,0 & 0\,0\,1 & 0\,0\,1 \end{array}\right)$$

Ce code $\mathcal{C}$ est la somme directe des codes binaires C_i, pour $1 \leq i \leq 3$, de matrices génératrices respectives :

$G_1 = \begin{pmatrix} 1\,0\,0\,1\,1 \\ 0\,1\,1\,0\,1 \end{pmatrix}$, $G_2 = \begin{pmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,1\,1\,1 \end{pmatrix}$ *et* $G_3 = \begin{pmatrix} 1\,0\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{pmatrix}$.

Le code C_1 a pour distance minimale 3. Celle des codes C_2 et C_3 est 2, la distance minimale de $\mathcal{C}$ est donc égale à 2.

On peut en déduire le théorème suivant :

Théorème 16. *Soit $\mathcal{C}$ un $\mathcal{F}$-code, de $\mathcal{L}$-matrice génératrice $\mathcal{G} = (\mathcal{I}_k|\mathcal{M})$. Le code $\mathcal{C}$ est un $\mathcal{R}$-code si et seulement si les matrices binaires correspondantes aux coefficients $\varphi_{i,j}$ de $\mathcal{M}$ sont diagonales.*

Démonstration. D'après la proposition 26, $\mathcal{C}$ est linéaire si et seulement s'il est somme directe des $e_i\mathcal{C}$, avec $e_{i,i} = 1$ et $e_{i,j} = 0$ pour $1 \leq i \neq j \leq m$. Ainsi les images binaires des éléments $\varphi_{i,j}$ sont des matrices diagonales. □

Les seuls codes binaires MDS de longueur s sont le code à répétions de paramètres $[s, 1, s]$ et son code dual, ainsi que le code de contrôle de parité de paramètres $[s, s-1, 2]$.

Les $\mathcal{R}$-codes MDS correspondent donc aux codes ayant pour projection un de ces deux codes. On en déduit que les seuls $\mathcal{R}$-codes MDS sont ceux dont l'image binaire a pour matrice génératrice l'une des deux matrices suivantes :

$$G = (\underbrace{I_m\, I_m \,...\, I_m}_{s}) \quad \text{ou} \quad G' = \begin{pmatrix} I_m & 0 & \dots & 0 & I_m \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & I_m & I_m \end{pmatrix}$$

5.6.2 Codes sur $\mathbb{F}_2[x]/f(x)$

Dans cette section on considère à nouveau l'anneau $\mathcal{A} = \mathbb{F}_2[x]/f(x)$ des polynômes binaires quotientés par un polynôme $f(x)$ de degré m. L'identification d'un polynôme de degré strictement plus petit que m à ses m coordonnées binaires font des $\mathcal{A}$-codes un cas particulier des $\mathcal{F}$-codes.

Nous ne reviendrons pas sur les résultats présentés dans la partie II de cette thèse, mais nous allons explorer les éventuelles décompositions de ces codes en utilisant les sous-anneaux de $\mathcal{A}$.

Si $f(x) = \prod_{i=1}^{t} f_i(x)^{j_i}$, $j_i \geq 1$ est la décomposition de $f(x)$ en polynômes irréductibles $f_i(x)$, l'étude de l'anneau $\mathcal{A}$ et des $\mathcal{A}$-codes se ramène à l'étude des projections sur les anneaux $\mathcal{A}_i = \mathbb{F}_2(x)/f_i(x)^{j_i}$ et des $\mathcal{A}_i$-codes. De nombreuses études ont été faites avec cette approche [[14], [13]].

Les principales propriétés de l'algèbre $\mathcal{A}$ sont les suivantes : l'anneau $\mathcal{A}$ est un anneau principal, les idéaux de $\mathcal{A}$ sont ceux générés par les diviseurs de $f(x)$, et les idéaux minimaux de $\mathcal{R}$ sont ceux générés par les éléments $h_i(x) = f(x)/f_i(x)$.

Nous allons considérer un cas particulier qui nous permettra par la suite de construire de bonnes matrices de diffusion cryptographiques à partir de matrices définies sur un alphabet plus petit. On suppose que $f(0) = 1$ c'est-à-dire que x n'est pas un facteur de $f(x)$, et que le polynôme $f(x)$ est sans facteur carré, c'est-à-dire que $f(x) = \prod_{i=1}^{t} f_i(x)$, $f_i(x)$ irréductibles distincts.

Les anneaux $\mathbb{F}(x)/f_i(x)$ sont alors des corps K_i qui sont des extensions de $\mathbb{F}_2$ de degré $m_i = deg(f_i(x))$. Dans cette situation, on sait que l'algèbre $\mathcal{A}$ est semi-simple et isomorphe au produit de corps $\prod_{i=1}^{t} K_i$.

Pour $i \in [1; t]$, on définit la projection p_i de $\mathcal{A}$ dans K_i par :
$p_i(g(x)) = g(x) \bmod f_i(x)$. On étend l'action de p_i au module $E = \mathcal{R}^s$ en faisant agir la projection composante par composante. L'image C_i du $\mathcal{R}$-code $\mathcal{C}$ par p_i est alors un code K_i-linéaire.

Le théorème suivant est un résultat bien connu.

Théorème 17. *Soit $f(x)$ un polynôme sans facteur carré vérifiant $f(0) = 1$. Le code $\mathcal{R}$-linéaire $\mathcal{C}$ est isomorphe à la somme directe de ses projections : $\mathcal{C} \simeq \oplus_{i=1}^{s} C_i$.*

Démonstration. La démonstration est essentiellement la même que celle de la proposition 26 en remplaçant les codes $e_i\mathcal{C}$ par les codes C_i. La reconstruction d'un mot c à partir de ses projections $c \pmod{f_i(x)}$ se faisant à l'aide du théorème des restes chinois. □

Le corollaire suivant relie la distance minimale de $\mathcal{C}$ à celle de ses projections :

Corollaire 2. *Sous les hypothèses du théorème 17, la distance minimale de $\mathcal{C} \neq \{0\}$ est le minimum des distances minimales non nulles d_i de ses projections C_i.*

En particulier, $\mathcal{C}$ est MDS si et seulement si tous les codes C_i sont MDS.

Démonstration. Soit $d(C_j) = min(d(C_i), 1 \leq i \leq s) = d$ et $u \in C_j$ avec $w(u) = d \neq 0$.

On peut construire un mot $c \in \mathcal{C}$ à partir de u et les élément nuls des autres codes à l'aide du théorème des restes chinois. Ce mot c a le même poids que u, c'est-à-dire d.

Réciproquement, le poids des projections de c sur les codes C_i est inférieur ou égal au poids de c, d'où le résultat.

□

Lorsqu'on regarde le cas des codes quasi-cycliques correspondant à $f(x) = x^m - 1$, si m est impair, on peut appliquer le théorème 17 puisque la décomposition de $f(x)$ est alors sans facteur carré. On peut remarquer que $x - 1$ est un facteur de $f(x)$, et donc, comme il n'existe pas de codes binaires MDS à part les codes triviaux, on ne peut pas construire de $\mathcal{R}$-codes quasi-cycliques MDS non triviaux. Ce résultat peut s'étendre facilement au cas m pair.

En pratique, nous utiliserons dans la dernière partie des codes MDS sur $\mathbb{F}_{2^{m/2}}$ pour construire des $\mathcal{R}$-codes sur $\mathbb{F}_2^m$.

Chapitre 6

Codes sur l'anneau $\mathcal{L}$

À la section 5.2.2, on a introduit une matrice d'encodage systématique d'un $\mathcal{F}$-code sous la forme d'une matrice $k \times s$ à coefficients dans l'anneau $\mathcal{L}$ des endomorphismes linéaires de $\mathcal{F} = \mathbb{F}_2^m$. Dans ce chapitre, on va au bout de cette approche en considérant les codes à coefficients directement dans l'anneau $\mathcal{L}$. Cet anneau étant non-commutatif, on a une notion de module à gauche et module à droite, ce qui fait que certains résultats classiques sur les codes linéaires se généralisent directement alors que d'autres deviennent plus délicats. Les codes considérés dans ce chapitre ne sont pas forcément systématiques

6.1 $\mathcal{L}$-codes

6.1.1 Définition des $\mathcal{L}$-codes

On rappelle que $\mathcal{L} = \mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2^m)$ est l'anneau non commutatif des endomorphismes $\mathbb{F}_2$-linéaires de $\mathcal{F} = \mathbb{F}_2^m$, et que sa deuxième loi (la multiplication) est la loi de composition des endomorphismes. Pour des raisons de cohérences avec les notations des matrices génératrices, pour $a \in \mathcal{F}$, φ et $\psi \in \mathcal{L}$, on pose :

$$a\psi\varphi = (\psi\varphi)(a) = \varphi(\psi(a)) = a(\varphi \circ \psi).$$

Par analogie avec la définition d'une matrice $\mathcal{L}$-génératrice donnée à la section 5.2.2, on peut définir un code $\mathcal{L}$-linéaire à gauche de la manière suivante :

Définition 33. *Un $\mathcal{L}$-code $\mathcal{C}$ (ou bien un code $\mathcal{L}$-linéaire à gauche) de longueur s sur $\mathcal{L}$ est un sous-module à gauche de $\mathcal{L}^s$.*

Autrement dit, il s'agit d'une partie de $\mathcal{L}^s$ stable par addition et par multiplication à gauche (loi de composition à droite) par un endomorphisme de $\mathcal{L}$.

De la même manière on peut définir un $\mathcal{L}$-code linéaire à droite. D'un point de vue pratique, ce sont les sous-modules à gauche qui correspondent avec la notion de $\mathcal{F}$-code.

Dans la suite, la notion de $\mathcal{L}$-code sans davantage de précisions désigne uniquement les sous-modules à gauche.

Le théorème suivant met en évidence la correspondance entre les $\mathcal{L}$-codes et les $\mathcal{F}$-codes additifs.

Théorème 18. *Soit $\mathcal{C}$ un $\mathcal{L}$-code linéaire de longueur s. L'ensemble*

$$\mathcal{C} = \{a\varphi = (\varphi_1(a), \varphi_2(a), \ldots, \varphi_s(a)) \ \in \ E | \forall a \in \mathcal{F} \text{ et } \forall \varphi \in \mathcal{C}\}$$

est un $\mathcal{F}$-code. Réciproquement, si $\mathcal{C}$ est un $\mathcal{F}$-code, l'ensemble

$$\mathcal{C} = \{\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_s) \in \mathcal{L}^s | \forall a \in \mathcal{F}, \ a\varphi \in \mathcal{C}\}$$

est un $\mathcal{L}$-code. De plus $\mathcal{C}$ et $\mathcal{C}$ ont la même distance minimale.

Démonstration. La correspondance est évidente par une simple vérification. Montrons l'égalité des distance minimales :
Soit $\varphi \in \mathcal{C}$ un s-uplet de $\mathbb{F}_2$-endomorphisme de $\mathcal{L}$ de poids minimum $d_{\mathcal{C}}$, et c un mot du code $\mathcal{C}$, alors il existe un élément a de $\mathbb{F}$ tel que $c = a\varphi$, alors $w(c) \leq d_{\mathcal{C}}$, ce qui implique que : $d_{\mathcal{C}} \leq d_{\mathcal{C}}$.

D'autre part si on prend $c = (c_1, \ldots, c_s)$ un mot de $\mathcal{C}$. On construit l'élément $\varphi' = (\varphi'_1, \ldots, \varphi'_s)$ de $\mathcal{L}^s$, telles que les matrices binaires des φ'_i, ont toutes la première ligne égale à c_i, et les autres lignes sont nulles.

On remarque que $a\varphi' = a_1 c$, alors les images par φ' de $a \in \mathcal{F}$ est un $\mathbb{F}_2$-espace vectoriel de dimension 1 généré par c, ce qui implique que φ' est un élément de $\mathcal{C}$. De plus $w(\varphi') = w(c)$. En choisissant c de poids minimal $d_{\mathcal{C}}$, on en déduit $d_{\mathcal{C}} \leq d_{\mathcal{C}}$.

En conséquence $d_{\mathcal{C}} = d_{\mathcal{C}}$. □

En suivant les notations et résultats de la section 5.2, on vérifie facilement que, si $\mathcal{C}$ est un $\mathcal{F}$-code systématique de pseudo-dimension k, alors le $\mathcal{L}$-code $\mathcal{C}$ correspondant est un $\mathcal{L}$-module de rang k, et il admet une matrice génératrice systématique.

Réciproquement, si $\mathcal{C}$ est de rang k et admet une matrice génératrice systématique, alors $\mathcal{C}$ est un $\mathcal{F}$-code systématique de pseudo-dimension k.

6.1.2 Dualité des $\mathcal{L}$-codes

La notion de $\mathcal{F}$-code ne permet pas d'introduire une dualité prenant en compte la structure en blocs de bits de taille m. Les $\mathcal{L}$-codes ayant une structure de module, il est naturel de s'intéresser à une éventuelle dualité. Pour cela, il faut généraliser la notion de produit scalaire.

$\mathcal{L}$-produit scalaire

Soient φ et ψ des éléments de $\mathcal{L}^s$ et $\lambda \in \mathcal{L}$ un "scalaire". On pose

$$< \varphi, \psi >= \sum_{i=1}^{s} \varphi_i \psi_i = \sum_{i=1}^{s} \psi_i \circ \varphi_i \in \mathcal{L}$$

On définit aussi les produits à gauche et à droite par le scalaire λ :

$\lambda\varphi = (\lambda\varphi_1, \ldots, \lambda\varphi_s)$ et $\varphi\lambda = (\varphi_1\lambda, \ldots, \varphi_s\lambda)$.

Soient $\varphi, \varphi', \psi, \psi'$ de $(\mathcal{L}^s)^4$, la bilinéarité de ce produit scalaire est donnée par une linéarité de module à gauche et à droite :

$$< \varphi + \varphi', \psi >=< \varphi, \psi > + < \varphi', \psi > .$$

$$< \varphi, \psi + \psi' >=< \varphi, \psi > + < \varphi, \psi' > .$$

$$< \lambda\varphi, \psi >= \lambda < \varphi, \psi > .$$

$$< \varphi, \psi\lambda >=< \varphi, \psi > \lambda.$$

Ce produit scalaire est non dégénéré, à savoir que si pour un φ fixé de $\mathcal{L}^s$, et pour tout ψ de $\mathcal{L}^s$ on a $< \varphi, \psi >= 0$ alors $\varphi = 0$, de même pour $< \psi, \varphi >= 0$.

Définition 34. *Soit $\mathcal{C}$ un $\mathcal{L}$-code, son dual $\mathcal{C}^\perp$ est le sous-ensemble de $\mathcal{L}^s$ défini par :*

$$\mathcal{C}^\perp = \{\psi \in \mathcal{L}^s | < \varphi, \psi >= 0, \forall\varphi \in \mathcal{C}\}.$$

A priori, le dual $\mathcal{C}^\perp$ n'est pas un module à gauche, ainsi on ne peut pas lui associer un $\mathcal{F}$-code. Le dual a cependant des propriétés liées à la structure de module énoncées dans le théorème suivant :

Théorème 19. *Soit $\mathcal{C}$ un $\mathcal{L}$-code (c'est-à-dire un $\mathcal{L}$-sous-module à gauche) de rang k sur $\mathcal{L}$. Le code dual $\mathcal{C}^\perp$ de $\mathcal{C}$ est un $\mathcal{L}$-sous module à droite de rang $s - k$.*

Démonstration. Si ψ et ψ' sont des éléments de $\mathcal{C}^\perp$, alors pour tout $\varphi \in \mathcal{C}$, $< \varphi, \psi + \psi' >=< \varphi, \psi > + < \varphi, \psi' >= 0$.

De même, pour $\lambda \in \mathcal{L}$ et $\psi \in \mathcal{C}$, $< \varphi, \psi\lambda >=< \varphi, \psi > \lambda = 0$ pour tout $\varphi \in \mathcal{C}$.

Le rang de $\mathcal{C}^\perp$ s'obtient en utilisant le fait que le produit scalaire est non dégénéré.

□

Proposition 27. *Soit $\mathcal{G}$ une $\mathcal{L}$-matrice génératrice d'un $\mathcal{L}$-code $\mathcal{C}$, et $\mathcal{H}$ une $\mathcal{L}$-matrice génératrice à droite de son dual $\mathcal{C}^\perp$ (les lignes forment un système générateur de module à droite $\mathcal{C}^\perp$). On a alors $\mathcal{G}\mathcal{H}^T = 0$. Réciproquement, si une matrice $\mathcal{H}$ génère un sous-module à droite de rang $s - k$ et satisfait l'équation $\mathcal{G}\mathcal{H}^T = 0$, alors $\mathcal{H}$ est une $\mathcal{L}$-matrice génératrice à droite de $\mathcal{C}^\perp$.*

Démonstration. Ces résultats s'obtiennent directement en utilisant le rang du dual et le fait que les coefficients de la matrice $\mathcal{G}\mathcal{H}^T$ ne sont rien d'autre que les produits scalaires des lignes de $\mathcal{G}$ et $\mathcal{H}$. □

Il faut noter que la condition $\mathcal{G}\mathcal{H}^T = 0$ n'entraîne pas $\mathcal{H}\mathcal{G}^T = 0$.

On a cependant la notion de matrice de contrôle :

Corollaire 3. *Si $\mathcal{H}$ est une matrice dont les lignes engendrent $\mathcal{C}^\perp$, alors $c \in \mathcal{C}$ si et seulement si $c.\mathcal{H}^T = 0$.*

De manière identique aux codes linéaires sur les corps finis, il est facile de construire une matrice de contrôle à partir d'une matrice génératrice systématique du code $\mathcal{C}$.

Proposition 28. *Soit $\mathcal{C}$ un $\mathcal{L}$-code systématique de longueur s, et $\mathcal{G} = (\mathcal{I}_k|\mathcal{M})$ sa matrice génératrice. La matrice $\mathcal{H} = (\mathcal{M}^T|\mathcal{I}_{(s-k)})$ est une matrice de contrôle pour $\mathcal{C}$. Elle est ainsi une matrice génératrice de son dual $\mathcal{C}^\perp$.*

Démonstration. Il suffit de vérifier que $\mathcal{G}\mathcal{H}^T = 0$, et que le rang de $\mathcal{H}$ est $s - k$. □

On note bien que la matrice transposée de $\mathcal{M}$ est la matrice construite en transposant les éléments de la matrice $\mathcal{M}$, et qu'elle n'est pas égale à la transposée de sa matrice image binaire. Le théorème suivant est un équivalent au [[26], chap. 1, théorème 10], qui décrit le lien entre l'indépendance des colonnes de la matrice de contrôle d'un code et sa distance minimale.

Théorème 20. *Soit $\mathcal{C}$ un $\mathcal{F}$-code un et $\mathcal{H}$ une $\mathcal{L}$-matrice de contrôle de $\mathcal{C}$. Le code $\mathcal{C}$ a une distance minimale égale à d, si et seulement si chaque ensemble de $d-1$ colonnes de $\mathcal{H}$ définit une application linéaire de rang $d-1$, et de plus, s'il existe un ensemble de d colonnes de $\mathcal{H}$ correspondant à une application linéaire de rang strictement plus petit que d.*

Démonstration. La démonstration est similaire à celle de [[26], chap. 1, théorème 10]. La seule différence provient du fait que l'indépendance linéaire des colonnes est remplacée par le fait que l'application correspondant aux colonnes choisies est injective, et donc de noyau nul. □

6.1.3 Dualité binaire des $\mathcal{L}$-codes

Dans la section 5.3.1, nous avons introduit la notion d'image binaire d'un $\mathcal{F}$-code additif. On peut alors naturellement construire son dual binaire. L'objet de cette section est d'étudier les relations existantes entre le dual de l'image binaire d'un $\mathcal{L}$-code et son dual relativement à la structure de $\mathcal{L}$-module. Pour cela, nous allons introduire un nouveau produit scalaire "Hermitien" sur $\mathcal{L}^s$.

Soit ϕ un endomorphisme de $\mathcal{L}$. On associe à ϕ sa matrice binaire $\mathcal{M}_\phi$ relative à la base canonique de $\mathcal{F}$. La transposée de ϕ est alors l'application linéaire $\phi^T \in \mathcal{L}$ dont la matrice binaire associée est M_ϕ^T.

On peut alors définir sur $\mathcal{L}^s$ un "produit scalaire Hermitien" de la manière suivante : si φ et ψ sont des éléments de $\mathcal{L}^s$, alors $< \varphi, \psi >_T = \sum_{i=1}^{s} \varphi_i \psi_i^T \in \mathcal{L}$.

On peut remarquer que, pour tout φ et $\psi \in \mathcal{L}^s$ et pour tout $\lambda \in \mathcal{L}$, on a $< \lambda\varphi, \psi >_T = \lambda < \varphi, \psi >_T$ et $< \varphi, \lambda\psi >_T = < \varphi, \psi >_T \lambda^T$.

On définit le dual binaire d'un $\mathcal{L}$-code comme suit :

Définition 35. *Soit $\mathcal{C}$ un $\mathcal{L}$-code linéaire. Le dual binaire $\mathcal{C}^{\perp *}$ de $\mathcal{C}$ est le sous-ensemble de $\mathcal{L}^s$ défini par :*

$$\mathcal{C}^{\perp *} = \{\psi \in \mathcal{L}^s | < \varphi, \psi >_T = 0, \ \forall \varphi \in \mathcal{C}\}$$

Théorème 21. *Soit $\mathcal{C}$ un $\mathcal{L}$-code systématique linéaire de rang k. Le dual binaire $\mathcal{C}^{\perp *}$ de $\mathcal{C}$ est un $\mathcal{L}$-sous-module linéaire à gauche de $\mathcal{L}^s$ de rang $s-k$, c'est-à-dire un $\mathcal{L}$-code systématique.*

Démonstration.

La démonstration du $\mathcal{L}$-sous module à gauche vient directement du fait que

$$< \varphi, \lambda\psi >_T = < \varphi, \psi >_T \lambda^T$$

ce qui implique en particulier que, si $< \varphi, \psi >_T = 0$, alors $< \varphi, \lambda\psi >_T = 0$, pour tout $\lambda \in \mathcal{L}$, on en déduit que $\mathcal{C}^{\perp *}$ est un sous-module à gauche.

$\mathcal{C}$ est un code systématique, on suppose que $\mathcal{G} = (\mathcal{I}_k|\mathcal{M})$ est sa matrice génératrice de taille $k \times s$, la matrice $\mathcal{H} = (\mathcal{M}^T|\mathcal{I}_{s-k})$ est la matrice génératrice du code dual binaire $\mathcal{C}^{\perp *}$, ainsi $s-k$ est son rang.

□

Pour éclaircir la relation entre les deux types de dualité, on introduit la notation suivante :

si $\mathcal{M} = (\varphi_{i,j})$ est une matrice à coefficients dans $\mathcal{L}$, on note $\mathcal{M}^* = (\varphi_{i,j}^T)$ la matrice transposée des applications de $\mathcal{M}$, obtenue en remplaçant chaque entrée de la matrice par son application transposée.

On note qu'on ne transpose pas la matrice elle même, mais ses coefficients uniquement. De la même manière si $\varphi = (\varphi_1, \ldots, \varphi_s)$ est un élément de $\mathcal{L}^s$, on pose $\varphi^* = (\varphi_1^T, \ldots, \varphi_s^T)$.

Proposition 29.

Soit $\varphi \in \mathcal{L}^s$, φ est un élément de $\mathcal{C}^\perp$, si et seulement si φ^* est un élément de $\mathcal{C}^{\perp *}$.

Démonstration. Cette proposition est une conséquence directe de la définition 34 et de la définition 35. □

On obtient directement le corollaire suivant :

Corollaire 4. *Une matrice $\mathcal{H}$ est une matrice génératrice du $\mathcal{L}$-code $\mathcal{C}^\perp$, si et seulement si la matrice à droite $\mathcal{H}^*$ est une matrice génératrice du $\mathcal{L}$-code $\mathcal{C}^{\perp *}$ "dual binaire" de $\mathcal{C}$. En particulier, si $\mathcal{G} = (\mathcal{I}_k|\mathcal{M})$ est la matrice génératrice de $\mathcal{C}$ sous la forme systématique, alors $\mathcal{H}^* = (\mathcal{M}^{T*}|\mathcal{I}_r)$ est une matrice génératrice de $\mathcal{C}^{\perp *}$.*

La proposition suivante montre que les notions de "dual binaire" pour les $\mathcal{L}$-codes et de dualité binaire définie à la section 2.3.2 sont cohérentes.

Proposition 30. *Soit $\mathcal{C}$ un $\mathcal{F}$-code systématique et $\mathcal{C}$ le $\mathcal{L}$-code associé. On note par C l'image binaire de $\mathcal{C}$ (C est donc un code binaire de paramètres $[ms; mk]$).*

Soit $C^\perp$ le code binaire dual de $\mathcal{C}$. L'image binaire du $\mathcal{F}$-code associée au $\mathcal{L}$-code $\mathcal{C}^{\perp *}$ est le code $C^\perp$, dual binaire de $\mathcal{C}$.

Démonstration.

Pour φ, $\psi \in \mathcal{L}^s$, on a $< \varphi, \psi > \in \mathcal{L}$. Le résultat est alors la conséquence directe de la relation $\mathcal{M}_{<\varphi,\psi>} = \sum_{i=1}^s \mathcal{M}_{\varphi_i} \mathcal{M}_{\psi_i}^T$. □

6.2 Codes linéaires sur un sous-anneau de $\mathcal{L}$

Le but de cette section est de se focaliser sur les $\mathcal{F}$-codes additifs dont la $\mathcal{L}$-matrice génératrice a ses coefficients dans certains sous-anneaux $\mathcal{R}$ de $\mathcal{L}$.

On peut étendre naturellement les résultats de la section 6.1 et définir les $\mathcal{R}$-codes systématiques en tant que $\mathcal{R}$-sous modules à gauche de $\mathcal{R}^s$. On peut définir la $\mathcal{R}$-dualité et la dualité binaire sur ces codes.

Il est à noter que, si $\mathcal{R}$ est commutatif, la notion de sous-module à gauche et à droite est la même, on a donc une notion de $\mathcal{F}$-codes duaux en tant que codes sur des blocs, par contre $\mathcal{C}^{\perp} \neq \mathcal{C}^{\perp *}$, le contre-exemple est celui des corps finis, où ces codes ne coïncident pas.

La coïncidence ne se fait que si les entrées de la $\mathcal{L}$-matrice génératrice sont symétriques. Par contre, dans le cas non-commutatif, le produit de 2 matrices symétriques n'est pas toujours symétrique.

6.2.1 Endomorphismes diagonaux

Un endomorphisme diagonal est un endomorphisme tel que sa matrice binaire est diagonale. On note par $\mathcal{D}$ l'anneau des endomorphismes diagonaux. Ce dernier est isomorphe à l'anneau $(\mathbb{F}_2^m, +, *)$. Les $\mathcal{F}$-codes correspondants sont exactement ceux introduits dans la section 5.6.1.

L'anneau $\mathcal{D}$ est commutatif, de plus ses éléments sont symétriques. Les notions de dualité binaire ou de $\mathcal{L}$-dualité se confondent. des

Dans l'optique de la recherche de codes MDS, ce cas particulier ne pourra pas donner de bons codes.

6.2.2 Sous-anneaux de $\mathcal{L}$ à générateur unique

Soit ψ un élément inversible de $\mathcal{L}$, et $\mathcal{P}(\psi) = \{P(\psi) = \sum_{i=0}^{deg(P(x))} p_i \psi^i\}$ le sous-anneau de $\mathcal{L}$ généré par ψ. Un certain nombre de travaux permettant de construire de bonnes matrices de diffusion pour la cryptographie, utilisent ce type de sous-anneau de $\mathcal{L}$. On pourra en particulier consulter [2] sur ce sujet.

L'anneau $\mathcal{P}(\psi)$ est commutatif, il admet donc une notion interne de $\mathcal{P}(\psi)$-dualité.

Soit $f(x)$ le polynôme minimal de ψ. L'anneau d'endomorphismes $\mathcal{P}(\psi)$ est alors isomorphe à $\mathbb{F}_2[x]/f(x)$. Nous retrouvons alors les résultats de la section 5.6.1.

Si $f(x)$ est irréductible, la $\mathcal{P}(\psi)$-dualité est équivalente à la dualité des codes sur le corps fini $\mathbb{F}_2[x]/f(x)$. Dans ce cas cette dualité est différente de la dualité binaire.

On peut remarquer que, si ψ est un endomorphisme symétrique, alors tous les endomorphismes de $\mathcal{P}(\psi)$ sont symétriques. Il n'y a alors plus qu'une seule notion de dualité.

6.2.3 Endomorphismes blocs-diagonaux

Soient m' et m'' deux entiers non nuls tels que : $m = m' + m''$. Un élément $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$ peut être identifier par le couple (x', x'') avec $x' = (x_1, \ldots, x_{m'}) \in \mathbb{F}_2^{m'}$ et $x'' = (x_{m'+1}, \ldots, x_{m''}) \in \mathbb{F}_2^{m''}$.

On note par $\mathcal{L}'$ et $\mathcal{L}''$ les anneaux des endomorphismes linéaires de $E' = (\mathbb{F}_2^{m'})^s$ et $E'' = (\mathbb{F}_2^{m"})^s$. En utilisant les identifications précédentes, l'anneau $\mathcal{R}_{m',m''} = \mathcal{L}' \times \mathcal{L}''$ peut être considéré comme un sous-anneau de $\mathcal{L}$. Les endomorphisme de $\mathcal{R}_{m',m''}$ sont ceux dont les matrices sont diagonales par bloc de matrices, tel que le premier bloc est de taille m' et le deuxième est de taille m''.

En pratique, les $\mathcal{R}_{m',m''}$-codes sont construits à partir d'une somme directe d'un $\mathcal{L}'$-code et d'un $\mathcal{L}''$-code. Bien que cette construction ne soit pas très efficace au niveau des bits, cette méthode permet de construire de grandes matrices MDS à partir de petites matrices MDS, ce qui peut s'avérer intéressant au niveau implémentation. Les valeurs typiques de m' et m'' sont $m' = m''$, et alors $m = 2m'$.

Exemple 14. *Soit $\mathcal{G}$ une matrice génératrice d'un $\mathcal{R}_{m',m''}$-bloc code $\mathcal{C}$ de longueur 3 telle que :*

$$\mathcal{G} = \left(\begin{array}{cc|cc|cc} \mathcal{M}_{1,1} & 0 & \mathcal{M}_{1,2} & 0 & \mathcal{M}_{1,3} & 0 \\ 0 & \mathcal{M}'_{1,1} & 0 & \mathcal{M}'_{1,2} & 0 & \mathcal{M}'_{1,3} \\ \hline \mathcal{M}_{2,1} & 0 & \mathcal{M}_{2,2} & 0 & \mathcal{M}_{2,3} & 0 \\ 0 & \mathcal{M}'_{2,1} & 0 & \mathcal{M}'_{2,2} & 0 & \mathcal{M}'_{2,3} \end{array}\right).$$

Soient $\mathcal{G}_1 = \left(\begin{array}{c|c|c} \mathcal{M}_{1,1} & \mathcal{M}_{1,2} & \mathcal{M}_{1,3} \\ \hline \mathcal{M}_{2,1} & \mathcal{M}_{2,2} & \mathcal{M}_{2,3} \end{array}\right)$ *et* $\mathcal{G}_2 = \left(\begin{array}{c|c|c} \mathcal{M}'_{1,1} & \mathcal{M}'_{1,2} & \mathcal{M}'_{1,3} \\ \hline \mathcal{M}'_{2,1} & \mathcal{M}'_{2,2} & \mathcal{M}'_{2,3} \end{array}\right)$. *Ces matrices engendrent deux $\mathcal{L}$-codes $\mathcal{C}_1$ et $\mathcal{C}_2$.*

Le code $\mathcal{C}$ est en fait la somme directe des codes $\mathcal{C}_1$ et $\mathcal{C}_2$. En particulier le code $\mathcal{C}$ est MDS si et seulement si $\mathcal{C}_1$ et $\mathcal{C}_2$ sont MDS.

Quatrième partie

Matrices MDS et cryptographie

Partie IV : Matrices MDS et cryptographie

Introduction :

Cette partie utilise les résultats des chapitres précédents dans le but de construire des matrices MDS de diffusion. Ces dernières sont d'une grande importance dans la phase de permutation des systèmes cryptographiques symétriques basés sur l'architecture d'un réseau de permutation-substitution (SPN). Ce type de matrice assure une bonne résistances aux attaques classiques de la cryptanalyse. Pour des raisons d'optimisation des implémentation, nos matrices seront choisies avec des critères de symétrie, en particulier des matrices dyadiques et circulantes.

On commence cette partie par rappeler la relation existante entre un code MDS de rendement 1/2 et une matrice de diffusion optimale, et nous définissons d'une manière plus large la notion de matrice MDS de diffusion sur l'anneau non commutatif des endomorphismes de $\mathbb{F}_2^m$. Nous étudions les propriétés ainsi que l'équivalence de ces matrices. Nous donnons quelques exemples de construction de matrices MDS pour la diffusion. Dans la suite nous étudions les propriétés fondamentales des matrices circulantes et dyadiques, les résultats de cette étude seront utilisés dans la recherche exhaustive sur ces matrices structurées. Nous utilisons ensuite les résultats de cette recherche afin de construire des matrices MDS de diffusion optimales pour la cryptographie symétrique. Nous terminons cette partie par une construction d'une famille infinie des matrices MDS dyadiques à partir des codes de Reed Solomon généralisés. Nous montrons que cette construction est duale à celle obtenue à partir des codes de Cauchy dans [36].

Liste des principaux symboles utilisés dans la partie IV :

— $\mathcal{F} = (\mathbb{F}_2^m, +)$: un groupe additif.
— $\mathcal{F}$-code : un code additif systématique de longueur $s = 2k$ sur $\mathcal{F}$.
— $\mathcal{C}$: un $\mathcal{F}$-code.
— C : l'image binaire d'un $\mathcal{F}$-code $\mathcal{C}$.
— $n = sm = 2km$: la longueur du code C, image binaire du $\mathbb{F}$-code systématique $\mathcal{C}$.
— $\mathcal{L}$: l'anneau des endomorphisme de $\mathcal{F}$.
— $\mathcal{L}$-code : un code systématique de longueur s sur $\mathcal{L}$.
— $\mathcal{C}$: un $\mathcal{L}$-code.
— $\mathcal{M}$: une matrice carrée de taille k à coefficients dans $\mathcal{L}$.
— M^T : la transposée de l'image binaire de $\mathcal{M}$.
— M_φ : la matrice carrée $m \times m$ binaire de l'endomorphisme φ.
— M : la matrice binaire de taille $km \times km$ associé à la matrice $\mathcal{M}$.
— $\mathcal{M}_\varphi^T$: la transposée de la matrice $\mathcal{M}_\varphi$.
— φ^T : l'endomorphisme associe à la matrice $\mathcal{M}_\varphi^T$.
— $\mathcal{M}^*$: la matrice dont les coefficients sont les endomorphismes transposés de ceux de $\mathcal{M}$.
— $\mathcal{M}^{T*}$: la matrice transposée de $\mathcal{M}^*$.
— $w_b(x)$: le poids par bloc de taille m de x.
— $\mathcal{B}_d(M)$: le branche number différentiel de M.
— $\mathcal{B}_l(M)$: le branche number linéaire de M.
— $\mathbf{M}$: une matrice carrée à coefficients sur le corps fini $\mathbb{F}_{2^m}$.
— $circ(a_0, \ldots, a_{k_1})$: matrice circulante de première ligne $(a_0, \ldots, a_{k_1})$.
— $e_i = (0, \ldots, 1, \ldots, 0)$: le vecteur de longueur k, à coefficients dans $\mathcal{L}$, et tel que 1 est à la position i.
— S : la matrice de permutation circulante $circ(e_1)$.
— $\mathfrak{C}_k$: l'ensemble des matrices circulantes de taille k sur $\mathcal{L}$.
— $dyad(a_0, \ldots, a_{k_1})$: matrice dyadique de première ligne $(a_0, \ldots, a_{k_1})$.
— $\mathcal{P}_i$: la matrice de permutation $dyad(e_i)$.
— $\mathfrak{D}_k$: l'ensemble des matrices dyadiques de taille k sur $\mathcal{L}$.
— $w(M)$: le poids de Hamming de la matrice binaire M.

Chapitre 7

Codes MDS et cryptographie

Dans ce chapitre, nous présentons les matrices de diffusion MDS utilisées dans les chiffrements par blocs de type SPN sous leur forme la plus générale, c'est-à-dire comme des matrices d'endomorphismes à coefficients dans $\mathcal{L} = \mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2^m)$. Nous généralisons les liens connus entre les matrices de diffusion optimales et les codes MDS aux $\mathcal{F}$-codes MDS.

Nous précisons la notion d'équivalence entre ces matrices de diffusion MDS. Nous terminons en donnant des exemples de constructions de matrices MDS qui utilisent les résultats des chapitres précédents.

7.1 Matrices de diffusion MDS

7.1.1 Réseaux de substitution-permutation

Dans le domaine de la cryptologie, notamment le chiffrement par bloc, un réseau de permutation-substitution (SPN pour "Substitution Permutation Network") est une architecture de chiffrement itérative, tel que chaque tour est composé de trois opérations :

- La première est l'introduction de la clé de tour dans le chiffrement. Il s'agit en général d'un simple XOR entre la clé et l'état du registre.
- La deuxième est une application non-linéaire de substitution, qui a pour rôle de compliquer la relation entre le clair, le chiffré et la clé. Elle est en général réalisée par des S-boxes, qui, pour des raisons d'efficacité, agissent sur des blocs de taille m, typiquement de 8 bits, ou 4 bits en cryptographie légère.
- La troisième opération est la permutation ou diffusion. Elle est réalisée en général par une application linéaire et a pour but de diffuser la non-linéarité entre les blocs en sortie des S-boxes.

Suivant les deux critères introduits par Claude Shannon dans son article [41] sur le principe de chiffrement, la substitution assure la confusion, tandis que la permutation assure la diffusion.

Un des exemples les plus connus des systèmes de chiffrement basés sur cette architecture est celui du chiffrement par bloc AES (Advanced Encryption

Standard) [16]. La confusion est réalisée par des S-boxes de taille $m = 8$. C'est l'opération SubBytes de l'AES. La diffusion quant à elle, ne peut pas s'appliquer sur l'état interne complet, puisqu'il faudrait utiliser une matrice binaire de taille 256. Elle se décompose donc en deux parties, la première appelée ShiftRows, est une simple permutation des blocs. La deuxième MixColumns agit en parallèle sur 4 blocs de 8 bits. C'est cette deuxième opération qui utilise une matrice directement dérivée des codes MDS et, conjointement avec l'action des Sboxes, assure la résistance aux attaques linéaires et différentielles.

Notre intérêt pour cette architecture concerne la phase de diffusion linéaire entre les blocs.

D'une manière formelle, si on considère k blocs de m bits en entrée de la phase de diffusion, on note cette entrée $x = (x_1, ..., x_k) \in (\mathbb{F}_2^m)^k$, on utilise soit une matrice de diffusion M binaire de taille $km \times km$, soit une matrice par bloc $\mathcal{M}$ de taille $k \times k$, où les entrées sont soit des endomorphismes de $\mathcal{L}$, soit les matrices binaires $m \times m$ correspondantes.

Pour respecter les conventions utilisées en théorie des codes, la sortie est alors $y = xM$ ou bien $y = x\mathcal{M}$, selon que l'on se place dans $\mathbb{F}_2^{mk}$ ou $(\mathbb{F}_2^m)^k$.

On rappelle que, si φ est un endomorphisme linéaire de $\mathcal{L}$, φ^T désigne l'endomorphisme transposé, c'est-à-dire l'élément de $\mathcal{L}$ dont la matrice image binaire est la matrice transposée de celle de φ : $M_{\varphi^T} = M_\varphi^T$.

La notation $\mathcal{M}^*$ désigne la matrice dont les coefficients sont les endomorphismes transposés de ceux de $\mathcal{M}$.

Il est important de signaler que $\mathcal{M}^*$, n'est pas la transposée $\mathcal{M}^T$ de $\mathcal{M}$: si $\mathcal{M} = (\varphi_{i,j})$, alors $\mathcal{M}^* = (\varphi_{i,j}^T)$ et $\mathcal{M}^T = (\varphi_{j,i})$. On note par $\mathcal{M}^{T*}$ la matrice $(\mathcal{M}^*)^T = (\mathcal{M}^T)^* = (\varphi_{j,i}^T)$.

On vérifie directement que, si M est la matrice binaire associée à $\mathcal{M}$, alors M^T est la matrice binaire associée à $\mathcal{M}^{T*}$.

7.1.2 Branch number

Le "branch number" d'une matrice de diffusion est une quantité qui mesure sa résistance contre les attaques linéaire et différentielle. On rappelle que $w_b(x)$ désigne le poids par blocs de taille m des éléments x et y de $\mathcal{F}^k$.

Les définitions ci-dessous sont tirées du livre [16] donnant les spécifications de l'AES.

Définition 36. *Soit M une matrice binaire de diffusion de taille $km \times km$ agissant sur k blocs de taille m.*

- *Le branch number différentiel de M est :*
  $\mathcal{B}_d(M) = min\{w_b(x) + w_b(xM) | x \in E,\ x \neq 0\}$.
- *Le branch number linéaire de M est :*
  $\mathcal{B}_l(M) = min\{w_b(x) + w_b(xM^T) | x \in E,\ x \neq 0\}$.

On remarque que cette définition du branch number est donnée au niveau de la matrice binaire. Si on veut l'écrire au niveau des matrices par blocs $\mathcal{M}$, il faut prendre la matrice associée à la transposée binaire dans la définition du branch number linéaire, c'est-à-dire la matrice que l'on a noté $\mathcal{M}^{T*}$.

L'objectif de sécurité consiste à construire des matrices de diffusion ayant des branch numbers linéaires et différentiels les plus grands possibles.

Ces définitions du branch number ont une interprétation immédiate en terme de théorie des $\mathcal{F}$-codes (cf. chapitre 5).

Nous donnons ci-après les définitions du branch number reformulées dans ce contexte.

Définition 37. *Soit $\mathcal{M}$ une matrice de diffusion de taille k sur des blocs de taille m. Soit $\mathcal{C}$ le $\mathcal{F}$-code additif systématique de matrice génératrice $(\mathcal{I}_k|\mathcal{M})$.*

- *Le branch number différentiel de $\mathcal{M}$ est la distance minimale (par bloc) du $\mathcal{F}$-code $\mathcal{C}$.*
- *le branch number linéaire de $\mathcal{M}$ est la distance minimale (par bloc) de son dual binaire $\mathcal{C}^{\perp *}$.*

L'équivalence entre les deux définitions du branch number vient directement du fait que les mots du code $\mathcal{C}$ sont exactement ceux de la forme $(x, x\mathcal{M})$ pour $x \in (\mathbb{F}_2^m)^k$. Le minimum des poids dans la définition de $\mathcal{B}_d(\mathcal{M})$ correspond bien à la distance minimale du code $\mathcal{C}$.

Le branch number linéaire, $\mathcal{B}_l$ correspond à la distance minimale du $\mathcal{F}$-code additif généré par $(\mathcal{I}_k|\mathcal{M}^{T*})$, qui est équivalent par permutation au code $\mathcal{C}^{\perp *}$ généré par la matrice $(\mathcal{M}^{T*}|\mathcal{I}_k)$.

En utilisant la théorie des codes correcteurs d'erreurs, on retrouve facilement quelques résultats donnés dans [16].

Proposition 31. *Si $\mathcal{M}$ est une matrice de diffusion sur k blocs, son branch number différentiel et son branch number linéaire sont bornés par : $k+1$.*

En effet, le code associé est un code de paramètres $[n = 2k, k]$. Sa distance minimale vérifie la borne de Singleton : $d \leq n - k + 1 = k + 1$.

De plus, le branch number différentiel est optimal lorsque $\mathcal{C}$ est MDS. On verra au théorème 22 que $\mathcal{C}$ est MDS si et seulement si $\mathcal{C}^{\perp *}$ est MDS. Du coup $\mathcal{M}$ a un branch number différentiel optimal si et seulement si $\mathcal{M}$ a un branch number linéaire optimal si et seulement si $\mathcal{C}$ est MDS.

7.1.3 Matrices de diffusion MDS

L'objectif de cette section est de définir de la manière la plus large possible la notion de matrices de diffusion MDS et de donner leurs premières propriétés.

Définition 38. *On considère une matrice carrée $\mathcal{M}$ de taille k à coefficients dans $\mathcal{L}$. On dit que la matrice $\mathcal{M}$ est une matrice de diffusion MDS si le $\mathcal{F}$-code $\mathcal{C}$ de matrice $\mathcal{L}$-génératrice $(\mathcal{I}_k|\mathcal{M})$ est MDS.*

Si M est la matrice $km \times km$ binaire associée à une matrice de diffusion MDS $\mathcal{M}$, on dit que M est une matrice MDS par blocs (de taille m).

Le code binaire C de matrice génératrice $(I_{km}|M)$ est alors appelé code MDS par blocs.

Le nombre $s = 2k$ désigne la longueur du $\mathcal{F}$-code $\mathcal{C}$, alors que $n = sm = 2km$ désigne la longueur du code binaire C.

La pseudo-dimension du $\mathcal{F}$-code MDS $\mathcal{C}$ est k, sa distance minimale est donc $d = k + 1$. La valeur d est aussi appelée distance minimale par bloc du code binaire C.

Le lemme suivant permet d'utiliser la représentation binaire et la notion de déterminant, alors que celle-ci n'existe pas sur l'anneau des matrices à coefficients dans $\mathcal{L}$.

Lemme 10. *Une matrice carrée $\mathcal{M}$ est inversible si et seulement si sa matrice image binaire associée M est inversible. De plus, l'image binaire de $\mathcal{M}^{-1}$ est M^{-1}.*

Démonstration. Ces propriétés découlent directement du fait que l'application $\mathcal{M} \mapsto M$, de l'anneau des matrices carrées de taille $k \times k$, à coefficients dans $\mathcal{L}$ vers l'anneau des matrices carrés binaires de taille $rm \times rm$ est un isomorphisme.

□

La proposition suivante est une conséquence directe du théorème 15 et de la définition 38.

Proposition 32. *Soit $\mathcal{M}$ une matrice carrée de taille k sur $\mathcal{L}$, la matrice $\mathcal{M}$ est MDS si et seulement si toute sous-matrice carrée de $\mathcal{M}$ est inversible.*

De manière équivalente, soit M une matrice binaire carrée de taille km. La matrice M est une matrice m-bloc MDS, si et seulement si les sous-déterminants pris par blocs de taille $m \times m$ de M sont non nuls.

Le résultat principal de cette section est le théorème suivant :

Théorème 22. *Soit $\mathcal{M}$ une matrice carrée de taille k sur $\mathcal{L}$, et M sa matrice binaire carrée associée. Les conditions suivantes sont équivalentes :*

1. *$\mathcal{M}$ est une matrice MDS.*
2. *$\mathcal{M}^{T*}$ est une matrice de diffusion MDS.*
3. *$\mathcal{M}^{-1}$ est une matrice de diffusion MDS.*
4. *M est une matrice de diffusion MDS par bloc.*
5. *M^T est une matrice de diffusion MDS par bloc.*
6. *M^{-1} est une matrice de diffusion MDS par bloc.*

Par abus de langage, lorsque le contexte est clair (en particulier lorsqu'on a affaire à une matrice carrée), une matrice de diffusion MDS $\mathcal{M}$ sera simplement appelée matrice MDS. On fera de même pour la notion de MDS par blocs.

Démonstration.

— Les équivalences $1 \Leftrightarrow 4$, $2 \Leftrightarrow 5$ et $3 \Leftrightarrow 6$, viennent directement de la définition 38.

— $1 \Leftrightarrow 2$ (et donc $4 \Leftrightarrow 5$) :
Supposons que $\mathcal{M}$ est une matrice MDS. Soit $\mathcal{B}$ une sous-matrice carrée de $\mathcal{M}^{T*}$ de taille l. On remarque que $\mathcal{B}^{T*}$ est une sous-matrice de $\mathcal{M}$, elle est donc inversible par hypothèse, et alors $det(\mathcal{B}^T) = 1$. De plus on sait que $det(\mathcal{B}) = det(\mathcal{B}^T)$, donc la $\mathcal{L}$-matrice $\mathcal{B}$ est inversible, et ainsi $\mathcal{M}^{T*}$ est MDS.

— $4 \Leftrightarrow 6$ (et donc $1 \Leftrightarrow 3$) :
Soit M une matrice binaire MDS par blocs. On considère le code C généré par la matrice $G = (I_{km}|M)$. On sait que M est inversible, par la suite la matrice $G' = (M^{-1}|\mathcal{I}_{km})$ est aussi une matrice génératrice de C. En permutant les k premiers blocs et les k derniers de G, on obtient un code C' équivalent à C, et engendré par $(I_{km}|M^{-1})$. Ce code est également MDS par bloc, alors M^{-1} est MDS.

□

Dans le cas où les coefficients de M commutent entre eux, on a en plus la propriété suivante.

Proposition 33. *Supposons que tous les coefficients de $\mathcal{M}$ commutent entre eux, la matrice $\mathcal{M}$ est MDS si et seulement si $\mathcal{M}^T$ (respectivement $\mathcal{M}^*$) est MDS.*

Démonstration. Puisque l'on a la commutativité entre les éléments de $\mathcal{M}$, et en tirant profit de la proposition 32, alors, pour toute sous-matrice carrée $\mathcal{B}$ de $\mathcal{M}$, $det_{\mathcal{L}}(\mathcal{B}^T) = det_{\mathcal{L}}(\mathcal{B})^T$. L'élément $\varphi = det_{\mathcal{L}}(\mathcal{B}) \in \mathcal{L}$ est inversible si et seulement si $\varphi^T = det_{\mathcal{L}}(\mathcal{B})^T$ est inversible, ce qui démontre la proposition. □

7.1.4 Équivalence des matrices MDS

On a vu dans la section 5.5 que la distance par bloc des $\mathcal{L}$-codes est invariante par l'action du groupe monomial $Mon_{\mathcal{L}}$. Ce groupe étant engendré par les permutations du support et l'action d'éléments du groupe linéaire $GL(m, 2)$.

L'objectif de cette section est d'utiliser ces résultats pour déterminer une notion d'équivalence des matrices de diffusion MDS.

Considérons d'abord le cas des permutations. Une matrice MDS $\mathcal{M}$ est associée au $\mathcal{L}$-code $\mathcal{C}$ engendré par la matrice $\mathcal{G} = (\mathcal{I}_k|\mathcal{M})$. Pour préserver cette structure, on considère les permutations qui préservent la partie information de la partie redondance.

Soient P_1 et P_2 deux matrices de permutations agissant sur k éléments et $P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$.

Si $\mathcal{C}$ est un code MDS, son image $\mathcal{C}'$ par la permutation P est MDS et a pour matrice génératrice $(P_1|\mathcal{M}P_2)$. En mettant cette matrice sous forme systématique, on obtient la matrice génératrice $\mathcal{G}' = (\mathcal{I}_k|\ P_1^{-1}\mathcal{M}P_2)$.

Nous avons ainsi démontré la proposition suivante :

Proposition 34. *Soient P_1 et P_2 deux matrices de permutations de taille k à coefficients dans $\mathcal{L}$. Une matrice de diffusion $\mathcal{M}$ est MDS si et seulement si la matrice de diffusion $\mathcal{M}' = P_1 \mathcal{M} P_2$ est MDS.*

En pratique, si on a une matrice de diffusion MDS $\mathcal{M}$, on ne change pas la propriété MDS en permutant les lignes et/ou les colonnes de cette matrice.

Définition 39. *Deux matrices de diffusion $\mathcal{M}$ et $\mathcal{M}'$ sont équivalentes par permutation s'il existe deux matrices de permutation P_1 et P_2 telles que $\mathcal{M}' = P_1 \mathcal{M} P_2$*

On considère maintenant la "multiplication scalaire", c'est-à-dire la multiplication de chaque coordonnées par des éléments inversibles de $\mathcal{L}$ (les éléments de $GL(m, 2)$). On considère donc une matrice diagonale $\mathcal{D}$ de taille $s = 2k$ dont les éléments de la diagonale sont $\lambda_1, \ldots, \lambda_s \in GL(m, 2)$.

De manière similaire à ce que l'on a fait pour les permutations, on décompose la matrice $\mathcal{D}$ en deux sous-blocs diagonaux $\mathcal{D}_1$ et $\mathcal{D}_2$ tels que $\mathcal{D} = \begin{pmatrix} \mathcal{D}_1 & 0 \\ 0 & \mathcal{D}_2 \end{pmatrix}$.

L'image par $\mathcal{D}$ du $\mathcal{L}$-code $\mathcal{C}$ est le $\mathcal{L}$-code engendré par la matrice génératrice $(\mathcal{D}_1 | \mathcal{M}\mathcal{D}_2)$. Sa matrice systématique est alors $\mathcal{G}' = (\mathcal{I}_k | \mathcal{D}_1^{-1} \mathcal{M} \mathcal{D}_2)$.

On en déduit la proposition suivante :

Proposition 35. *Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux matrices diagonales de taille k à coefficients diagonaux dans $GL(m, 2)$. Une matrice de diffusion $\mathcal{M}$ est MDS si et seulement si la matrice de diffusion $\mathcal{M}' = \mathcal{D}_1 \mathcal{M} \mathcal{D}_2$ est MDS.*

En pratique, si on a une matrice de diffusion $\mathcal{M}$ MDS, on ne change pas la propriété MDS en multipliant à droite les lignes de $\mathcal{M}$ et à gauche ses colonnes par des éléments du groupe linéaire $GL(m, 2)$.

Définition 40. *Deux matrices de diffusion $\mathcal{M}$ et $\mathcal{M}'$ sont équivalentes par multiplication scalaire s'il existe deux matrices diagonales $\mathcal{D}_1$ et $\mathcal{D}_2$ telles que $\mathcal{M}' = \mathcal{D}_1 \mathcal{M} \mathcal{D}_2$.*

On peut alors définir la notion plus générale de matrices de diffusion équivalentes.

Définition 41. *Deux matrices de diffusion $\mathcal{M}$ et $\mathcal{M}'$ sont équivalentes s'il existe deux matrices monomiales $\mathcal{B}_1$ et $\mathcal{B}_2$ de taille k à coefficients dans $\mathcal{L}$ telles que $\mathcal{M}' = \mathcal{B}_1 \mathcal{M} \mathcal{B}_2$.*

Corollaire 5. *Si $\mathcal{M}$ est une matrice de diffusion MDS, les matrices équivalentes à $\mathcal{M}$ sont MDS.*

7.2 Premiers exemples de constructions

L'objectif de cette section est de présenter quelques exemples simples de constructions de matrices MDS à partir de celles obtenues sur les corps finis.

7.2.1 Matrices de diffusion MDS sur $\mathbb{F}_{2^m}$

La méthode la plus simple pour construire des matrices de diffusion MDS est à partir des codes MDS sur les corps finis. La principale classe de codes MDS connue est celle des codes de Reed Solomon et de ses dérivés, en particulier les codes de Reed Solomon généralisés.

Les codes de Reed Solomon seront introduits en détail au chapitre 9. Le principe est de construire un code de Reed Solomon de dimension k et de longueur $s = 2k$ sur le corps fini $\mathbb{F}_{2^m}$, et ensuite de mettre sa matrice génératrice sous forme canonique $(\mathbf{I}_k|\mathbf{M})$. Il suffit alors d'interpréter la matrice de redondance $\mathbf{M}$ à coefficients dans $\mathbb{F}_{2^m}$ comme une matrice de diffusion binaire M MDS par blocs.

Il faut cependant remarquer que cette interprétation n'est pas unique et que le choix le plus efficace peut dépendre de l'implémentation.

Nous donnons un exemple d'une telle construction.

On considère le cas particulier $m = 3$ et $k = 3$. Si α est une racine primitive du corps fini $\mathbb{F}_{2^3}$, et on construit un code de Reed Solomon de paramètres [6,3,4], on obtient par la méthode décrite ci-dessus une matrice génératrice systématique $(\mathbf{I}_3|\mathbf{M})$, de C, où

$$\mathbf{M} = \begin{pmatrix} 1 & \alpha & \alpha^3 \\ 1 & \alpha^6 & \alpha^6 \\ 1 & \alpha^4 & \alpha^5 \end{pmatrix}$$

,

Supposons que le polynôme minimal de α soit x^3+x+1. Pour construire la matrice M binaire par blocs associée, on remplace α par la matrice compagnon du polynôme x^3+x+1 et les puissances de α par les puissances correspondantes de cette matrice. On obtient alors une première matrice de diffusion MDS :

$$M = \left(\begin{array}{c|c|c} 1\,0\,0 & 0\,1\,0 & 1\,1\,0 \\ 0\,1\,0 & 0\,0\,1 & 0\,1\,1 \\ 0\,0\,1 & 1\,1\,0 & 1\,1\,1 \\ \hline 1\,0\,0 & 1\,0\,1 & 1\,0\,1 \\ 0\,1\,0 & 1\,0\,0 & 1\,0\,0 \\ 0\,0\,1 & 0\,1\,0 & 0\,1\,0 \\ \hline 1\,0\,0 & 0\,1\,1 & 1\,1\,1 \\ 0\,1\,0 & 1\,1\,1 & 1\,0\,1 \\ 0\,0\,1 & 1\,0\,1 & 1\,0\,0 \end{array}\right)$$

Nous aurions pu prendre pour α une racine de $x^3 + x^2 + 1$, ce qui donne une autre matrice de diffusion binaire MDS par blocs :

$$M' = \left(\begin{array}{ccc} 1\,0\,0 & 0\,1\,0 & 1\,0\,1 \\ 0\,1\,0 & 0\,0\,1 & 1\,1\,1 \\ 0\,0\,1 & 1\,0\,1 & 1\,1\,0 \\ \hline 1\,0\,0 & 0\,1\,1 & 0\,1\,1 \\ 0\,1\,0 & 1\,0\,0 & 1\,0\,0 \\ 0\,0\,1 & 0\,1\,0 & 0\,1\,0 \\ \hline 1\,0\,0 & 1\,1\,1 & 1\,1\,0 \\ 0\,1\,0 & 1\,1\,0 & 0\,1\,1 \\ 0\,0\,1 & 0\,1\,1 & 1\,0\,0 \end{array}\right)$$

On peut construire un troisième exemple de matrice MDS binaire en choisissant la matrice symétrique $M_\alpha = \begin{pmatrix} 1\,0\,1 \\ 0\,0\,1 \\ 1\;1\,1 \end{pmatrix}$.

Son polynômes caractéristique est aussi $x^3 + x + 1$. Cette matrice engendre donc un sous-anneau de $\mathcal{L}$ qui est isomorphe au corps fini $\mathbb{F}_{2^3}$. La matrice de diffusion binaire MDS associée à la matrice $\mathcal{M}$ dans cette représentation est alors :

$$M'' = \left(\begin{array}{ccc} 1\,0\,0 & 1\,0\,1 & 0\,0\,1 \\ 0\,1\,0 & 0\,0\,1 & 0\,1\,1 \\ 0\,0\,1 & 1\,1\,1 & 1\,1\,0 \\ \hline 1\,0\,0 & 1\,1\,0 & 1\,1\,0 \\ 0\,1\,0 & 1\,0\,1 & 1\,0\,1 \\ 0\,0\,1 & 0\,1\,0 & 0\,1\,0 \\ \hline 1\,0\,0 & 1\,1\,1 & 0\,1\,1 \\ 0\,1\,0 & 1\,1\,0 & 1\,0\,0 \\ 0\,0\,1 & 1\,0\,0 & 1\,0\,1 \end{array}\right)$$

7.2.2 Un exemple non commutatif

Pour les valeurs $m = 3$, $k = 3$ et $s = 6$, on donne un exemple de matrice de diffusion MDS utilisant des endomorphismes symétriques, qui n'est pas équivalent aux constructions dérivées des corps finis ou des anneaux commutatifs. Cet exemple a été construit expérimentalement.

Soit $M = \begin{pmatrix} I_3 & M_{1,2} & M_{1,3} \\ I_3 & M_{2,2} & M_{2,3} \\ I_3 & M_{3,2} & M_{2,2} \end{pmatrix}$,

avec $M_{1,1} = M_{2,1} = M_{3,1} = I_3$, $M_{1,2} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $M_{1,3} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$,

$M_{2,2} = M_{3,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $M_{2,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ et $M_{3,2} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

La matrice M est une matrice de diffusion MDS par bloc, telle que toutes ses sous-matrices $M_{i,j}$ sont symétriques.

On peut remarquer que la matrice $M_{2,3}$ est d'ordre 2, et a pour polynômes minimal $x^2 + 1$.

Les matrices $M_{1,2}$ et $M_{2,2}$ sont d'ordre 3, et ont le même polynômes minimal $x^3 + 1$.

Les matrices $M_{1,3}$ et $M_{3,2}$ sont d'ordre 7, et leurs polynômes minimaux respectifs sont : $x^3 + x^2 + 1$ et $x^3 + x + 1$.

On note que ces 5 matrices ne commutent pas entre elles, et que l'anneau généré par ces matrices est l'anneau $\mathcal{L}$ des matrices binaires de taille 3×3.

7.2.3 Constructions itératives de matrices MDS

Endomorphismes blocs-diagonaux

Nous pouvons utiliser la méthode introduite au paragraphe 6.2.3 pour construire à partir de matrices MDS de taille m sur des corps finis, des matrices MDS de taille $k = 2m$.

En particulier on peut construire une matrice MDS par bloc de taille 6×6, à partir d'une matrice MDS de taille 3×3 construite sur les corps finis dans la section 7.2.1. Le fait que ces matrices agissent sur des blocs de 3 bits dans des blocs de 6 bits, n'affaiblit pas la diffusion de ces matrices, mais cela est conditionné par le fait que cette diffusion doit être appliquée après la confusion (les S-boxes) de ces blocs de 6 bits.

De manière générale, on applique la méthode des endomorphismes diagonaux de Section 6.2.1, à l'aide du produit tensoriel :

$$I_2 \otimes M_{\alpha^i} = \begin{pmatrix} M_{\alpha^i} & 0 \\ 0 & M_{\alpha^i} \end{pmatrix}$$

pour une matrice binaire M_{α^i} de $\mathcal{M}_3(\mathbb{F}_2)$ (l'ensemble des matrices carrées à coefficient dans $\mathbb{F}_2$).

Soit $M = (M_{i,j})$, une matrice carrée, et tel que ses coefficients $M_{i,j}$ sont des matrices MDS de taille 3×3 sur $\mathbb{F}_2$, et elles sont construites à partir des corps finis dans la section 7.2.1.

Alors la matrice $M^{(2)} = (I_2 \otimes M_{i,j})$, ainsi construite est une matrice MDS de taille 6×6.

Utilisation du théorème des restes chinois

Les matrices MDS sur des anneaux quotients étudiées dans la section 5.6.2 sont d'autres exemples qui permettent de construire des matrices MDS, en combinant des matrices MDS de petites tailles sur des corps finis.

Soit

$$\mathbf{M} = \begin{pmatrix} 1 & \alpha & \alpha^3 \\ 1 & \alpha^6 & \alpha^6 \\ 1 & \alpha^4 & \alpha^5 \end{pmatrix}$$

la matrice MDS donnée dans 7.2.1.

On pose $f_1(x) = x^3 + x + 1$, $f_2(x) = x^3 + x^2 + 1$ et $f(x) = f_1(x)f_2(x)$.

Leurs anneaux quotients correspondants :
$\mathcal{A}_1 = \mathbb{F}_2[x]/f_1(x)$, $\mathcal{A}_2 = \mathbb{F}_2[x]/f_2(x)$ et $\mathcal{A} = \mathbb{F}_2[x]/f(x)$.

Sachant que $\mathcal{A}_1$ et $\mathcal{A}_2$ sont isomorphes à $\mathbb{F}_8$ (puisque f_1 et f_2 sont irréductibles), alors la matrices $\mathbf{M}$ peut être vue comme une matrice $\mathbf{M}_1$ sur $\mathcal{A}_1$ et $\mathbf{M}_2$ sur $\mathcal{A}_2$ telle que :

$$\mathbf{M}_1 = \begin{pmatrix} 1 & x & x^3 \\ 1 & x^6 & x^6 \\ 1 & x^4 & x^5 \end{pmatrix} = \begin{pmatrix} 1 & x & x+1 \\ 1 & x^2+1 & x^2+1 \\ 1 & x^2+x & x^2+x+1 \end{pmatrix}$$

et

$$\mathbf{M}_2 = \begin{pmatrix} 1 & x & x^3 \\ 1 & x^6 & x^6 \\ 1 & x^4 & x^5 \end{pmatrix} = \begin{pmatrix} 1 & x & x+1 \\ 1 & x^2+x & x^2+x \\ 1 & x^2+x+1 & x+1 \end{pmatrix}.$$

La construction d'une matrice sur $\mathcal{A}$ utilise l'isomorphisme $\mathcal{A} \simeq \mathcal{A}_1\mathcal{A}_2$, en faisant appel au théorème des restes chinois de la manière suivante :

Soit $a_1(x)f_1(x) + a_2(x)f_2(x) = 1$ d'identité de Bézout sur $f_1(x)$ et $f_2(x)$. Au couple $(g_1(x), g_2(x)) \in \mathcal{A}_1 \times \mathcal{A}_2$ on associe le polynôme
$g(x) = a_2(x)f_2(x)g_1(x) + a_1(x)f_1(x)g_2(x) \in \mathcal{A}$.

Pour cet exemple les calculs donnent $a_1(x) = x$ et $a_2(x) = x + 1$.

Ainsi la matrice $\mathbf{M}$ sur $\mathcal{A}$ est $\mathbf{M} = xf_1(x)\mathbf{M}_1 + (x+1)f_2(x)\mathbf{M}_2$,

$$\mathbf{M} = \begin{pmatrix} 1 & x & x^6+x^5+x^4+1 \\ 1 & x^5+x^4+x^3+x^2 & x^5+x^4+x^3+x^2 \\ 1 & x^4+1 & x^6+x^4+x^3+x+1 \end{pmatrix}.$$

La matrice binaire est obtenue en remplaçant x par la matrice compagnon de $f(x)$ dans $\mathbf{M}$.

On note que la matrice compagnon de $f(x)$ est :

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

On a ainsi pu construire une matrice binaire MDS $\mathbf{M}$, de taille 18×18, par blocs de taille $m = 6$ à partir de matrices binaires MDS $\mathbf{M}_1$ et $\mathbf{M}_2$ de taille 9×9 par blocs de taille $m = 3$.

Chapitre 8

Matrices MDS structurées

Dans ce chapitre, nous nous intéressons aux matrices MDS de type circulantes ou dyadiques. Ces matrices sont efficaces pour les implémentations cryptographiques. Nous explorons leurs propriétés dans le cadre des matrices à coefficients dans $\mathcal{L} = \mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2^m)$.

La deuxième partie de ce chapitre explore les possibilités de la recherche exhaustive de matrices MDS structurées, en se limitant parfois à des sous-familles pour permettre de rendre cette recherche plus facile et obtenir des matrices avec de bonnes propriétés du point de vue implémentation, en particulier pour l'implémentation matériel.

8.1 Matrices MDS structurées pour la cryptographie

La finalité de cette étude est de faire une recherche la plus exhaustive possible sur des matrices MDS structurées, dans le but d'obtenir des matrices de diffusion intéressantes pour les applications en cryptographie symétrique. Les matrices structurées étudiées sont de type dyadiques et circulantes. La structure de ces matrices optimise le coût de l'implémentation logicielle et matérielle, et permet de tester plus facilement la propriété MDS.

En cryptographie symétrique, on s'intéresse particulièrement aux blocs de taille $m = 4$ ou $m = 8$ bits (pour un nombre de $k = 4$ ou $k = 8$ blocs). Il est possible de faire une recherche exhaustive sur $GL(m, 2)$ dans le cas $m = 4$ et $k = 4$, mais cela n'est plus possible pour $m = 8$ ou $k = 8$.

Dans l'objectif d'avoir une implémentation machine et logicielle efficace, Il est intéressant aussi de limiter cette recherche à des sous-ensembles tels que les matrices dérivées des corps finis $\mathbb{F}_{2^m}$, les matrices de poids faible, ou certaines matrices correspondant à des opérations simples proches des instructions machine, comme le XOR ou le décalage circulaire.

8.2 Matrices circulantes

Cette section explore les propriétés élémentaires des matrices MDS circulantes, ainsi que les classes d'équivalences sur ce type de matrices.

Nous considérons dans ce chapitre des matrices à coefficients dans $\mathcal{L}$. Les résultats s'appliquent directement aux cas des corps finis $\mathbb{F}_{2^m}$, des anneaux de type $\mathcal{A} = \mathbb{F}_2[x]/f(x)$, ainsi qu'aux sous-anneaux de $\mathcal{L}$ décrits dans les chapitres précédents. Il existe toujours un plongement de ces différents anneaux dans $\mathcal{L}$, au besoin en prenant la matrice binaire de taille $km \times km$ associée, qui sera toujours celle utilisée dans les applications cryptographiques.

8.2.1 Définitions

Définition 42. *Soit $\mathcal{M} = (\varphi_{i,j})$, $0 \leq i, j < k$, une matrice carrée de taille k à coefficients dans $\mathcal{L}$. La matrice $\mathcal{M}$ est dite circulante si, pour $i, j \in [0; k-1]$ et tout entier l, on a $\varphi_{i,j} = \varphi_{i+l,j+l}$, les sommes $i+l$ et $j+l$ étant calculées modulo k.*

Si $\mathcal{M}$ est une matrice circulante définie sur $\mathcal{L}$, on dit alors que sa matrice image binaire M est circulante par blocs (de taille m).

Une matrice circulante est entièrement définie par sa première ligne, les autres s'obtenant par décalage circulaire à droite de la ligne précédente. On note $circ(a_0, ..., a_{k-1})$ la matrice circulante obtenue à partir de la première ligne $(a_0, ..., a_{k-1})$.

8.2.2 Matrices de permutation circulantes

Il est immédiat de vérifier que les permutations circulante sur $\mathcal{L}^k$ sont exactement celles de la forme $circ(e_i)$ pour $0 \leq i < k$, où e_i est l'élément de $\mathcal{L}^k$ ayant l'identité en position i et 0 ailleurs.

Ce groupe est le groupe cyclique d'ordre k généré par la matrice :

$$circ(e_1) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \ddots & & \ddots & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix}$$

La matrice $circ(e_1)$ est notée par S (comme shift, c'est-à-dire décalage circulaire). Le lemme suivant caractérise les matrices circulantes en terme d'invariance par conjugaison par S.

Lemme 11. *Une matrice carrée $\mathcal{M}$ de taille k sur $\mathcal{L}$ est circulante, si et seulement si $S^{-1}\mathcal{M}S = \mathcal{M}$, ou bien de manière équivalente, $S\mathcal{M} = \mathcal{M}S$.*

Démonstration. Si on calcule $S^{-1}\mathcal{M}S = (\varphi'_{i,j})$, on obtient $\varphi'_{i,j} = \varphi_{i+1,j+1}$ pour $i, j \in [0; k-1]$. Par récurrence directe, en tenant compte de la définition 42, on en déduit que $\mathcal{M}$ est circulante.

Si $\mathcal{M}$ est une matrice circulante avec $\mathcal{M} = circ(\varphi_{1,1}, \varphi_{1,2}, \ldots, \varphi_{1,k})$, alors $S\mathcal{M} = circ(\varphi_{1,k}, \varphi_{1,1}, \ldots, \varphi_{1,(k-1)}) = \mathcal{M}S$, ainsi $S^{-1}\mathcal{M}S = \mathcal{M}$. □

On note par $\mathfrak{C}_k$ l'ensemble des matrices circulantes de taille k sur $\mathcal{L}$. Le théorème suivant donne la structure de $\mathfrak{C}_k$.

Théorème 23.

1. *L'ensemble $\mathfrak{C}_k$ est le sous-$\mathcal{L}$-module de $\mathcal{L}^k$ engendré par les matrice S^i, $0 \leq i < k$. Ce module est de rang k.*
2. *$(\mathfrak{C}_k, +, \times)$ (où $\times$ est la multiplication des matrices) est un sous-anneau de l'anneau des matrices $k \times k$ à coefficients dans $\mathcal{L}$. En particulier, si $\mathcal{M} \in \mathfrak{C}_k$ est inversible, alors $\mathcal{M}^{-1}$ est circulante.*
3. *Si les coefficients de deux matrices circulantes $\mathcal{M}$ et $\mathcal{M}'$ commutent, alors $\mathcal{M}\mathcal{M}' = \mathcal{M}'\mathcal{M}$.*

Démonstration.

1. Il s'agit d'une vérification directe, qui provient du fait que toute matrice circulante s'écrit de manière unique comme une combinaison linéaire à coefficients dans $\mathcal{L}$ des matrices de permutation circulantes.
2. Soient $\mathcal{M}$ et $\mathcal{N}$ deux matrices circulantes. En utilisant le lemme 11, on a $S^{-1}\mathcal{M}S = \mathcal{M}$ et $S^{-1}\mathcal{N}S = \mathcal{N}$, par conséquent $S^{-1}\mathcal{M}SS^{-1}\mathcal{N}S = \mathcal{M}\mathcal{N}$, ainsi $S^{-1}\mathcal{M}\mathcal{N}S = \mathcal{M}\mathcal{N}$, donc le produit de deux matrices circulante est une matrice circulante.

   Supposons maintenant que $\mathcal{M}$ soit inversible. Puisque l'anneau $\mathfrak{C}_k$ est fini, il existe deux entiers distincts $i, j \in \mathbb{N}$ tels que $\mathcal{M}^i = \mathcal{M}^j$. On pose $u = |i - j|$, alors $\mathcal{M}^u = I$, et puisque $\mathcal{M}$ est inversible $\mathcal{M}^{u-1} = \mathcal{M}^{-1}$ et $\mathcal{M}^{-1}$ est circulante.
3. Le produit de deux matrices circulantes étant circulante, pour démontrer l'égalité $\mathcal{M}\mathcal{M}' = \mathcal{M}'\mathcal{M}$ dans le cas de coefficients commutatifs, il suffit de comparer la première ligne de chaque produit, ou même la première ligne de l'une avec la première colonne de l'autre. On pose $\mathcal{M} = circ(\varphi_1, \ldots, \varphi_k)$ et $\mathcal{M}' = circ(\varphi'_1, \ldots, \varphi'_k)$,

   on peut donc se contenter de comparer la multiplication de la première ligne par la première colonne, et puisque les coefficients commutent alors $(\varphi_1\varphi'_1 + \varphi_2\varphi'_k + \varphi_3\varphi'_{k-1} + \ldots + \varphi_k\varphi'_2) = (\varphi'_1\varphi_1 + \varphi'_2\varphi_k + \varphi'_3\varphi_{k-1} + \ldots + \varphi'_k\varphi_2)$. Par conséquent $\mathcal{M}\mathcal{M}' = \mathcal{M}'\mathcal{M}$.

□

8.3 Matrices dyadiques

8.3.1 Définitions

Soit $\mathcal{M}$ une matrice carrée de taille $2t \times 2t$ sur un anneau quelconque. Et $\mathcal{M} = \begin{pmatrix} \mathcal{M}_{1,1} & \mathcal{M}_{1,2} \\ \mathcal{M}_{2,1} & \mathcal{M}_{2,2} \end{pmatrix}$ sa décomposition par blocs de taille $t \times t$.

Définition 43. *La matrice $\mathcal{M}$ est 2-blocs dyadique si on a les égalités : $\mathcal{M}_{1,2} = \mathcal{M}_{2,1}$ et $\mathcal{M}_{1,1} = \mathcal{M}_{2,2}$.*

Définition 44. *Soit $\mathcal{M}$ une matrice carrée de taille $k = 2^v$ sur $\mathcal{L}$. On définit de manière récursive la notion de matrice dyadique :*

- *Si $v = 0$, $\mathcal{M}$ est dyadique.*
- *Si $v > 0$, $\mathcal{M}$ est dyadique si et seulement si $\mathcal{M}$ est 2-blocs dyadiques et si chacune de ses sous-matrices $\mathcal{M}_{1,1}$ et $\mathcal{M}_{1,2}$ de taille $2^{v-1} \times 2^{v-1}$ est dyadique.*

Voici un exemple de matrice dyadique de taille 4×4 sur le corps fini $\mathbb{F}_{2^4}$:

Exemple 15. *Soit a une racine de $x^4 + x + 1$, tel que $\mathbb{F}_{16} = \mathbb{F}_2(a)$. Soit $\mathcal{M}$ la matrice définie par :*

$$\mathcal{M} = \begin{pmatrix} a^3 & a^{12} & 1 & a^{10} \\ a^{12} & a^3 & a^{10} & 1 \\ 1 & a^{10} & a^3 & a^{12} \\ a^{10} & 1 & a^{12} & a^3 \end{pmatrix}$$

On remarque que $\mathcal{M}_{1,1} = \mathcal{M}_{2,2} = \begin{pmatrix} a^3 & a^{12} \\ a^{12} & a^3 \end{pmatrix}$ et $\mathcal{M}_{1,2} = \mathcal{M}_{2,1} = \begin{pmatrix} 1 & a^{10} \\ a^{10} & 1 \end{pmatrix}$ et que ces sous-matrices sont bien dyadiques. La matrice $\mathcal{M}$ est donc dyadique.

On peut aussi vérifier en calculant tous les sous-déterminants de $\mathcal{M}$ que cette matrice est aussi MDS.

D'une manière analogue au cas des matrices circulantes, si $\mathcal{M}$ est une matrice dyadique à coefficients dans $\mathcal{L}$, on dira que sa matrice image binaire est dyadique par blocs (de taille m).

Dans la suite, on suppose que les matrices sont de taille $k = 2^v$ pour un entier v fixé. Comme pour les matrices circulante, une matrice dyadique est entièrement définie par sa première ligne. On note $dyad(a_0, \ldots, a_{k-1})$ la matrice dyadique dont la première ligne est $(a_0, \ldots, a_{k-1})$.

$$dyad(a_0, \ldots, a_{k-1}) = \begin{pmatrix} a_0 & a_1 & \ldots & a_{k-1} \\ a_1 & a_0 & \ldots & a_{k-2} \\ a_2 & a_3 & \ldots & a_{k-3} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k-1} & a_{k-2} & \ldots & a_0 \end{pmatrix}$$

8.3.2 Matrices de permutation dyadiques

De manière similaire au cas des matrices de permutation circulantes, les matrices de permutation dyadiques correspondent aux matrices dyadiques ayant un 1 sur la première ligne, les autres coefficients de cette ligne sont nuls.

Lemme 12. *Les matrices de permutation dyadiques sont exactement celles de la forme $\mathcal{P}_i = dyad(e_i)$, $0 \leq i < k$.*

Démonstration. Une matrice de permutation ayant un et un seul élément non nul, égal à 1 par ligne et par colonne, les seules candidates possibles sont les matrices $dyad(e_i)$. Il suffit alors de vérifier que ces matrices n'ont qu'un 1 par ligne et par colonne en utilisant le fait que toutes les lignes sont différentes et que les matrices dyadiques sont symétriques. □

Les matrices $\mathcal{P}_i$ sont d'ordre 2. En fait le groupe des permutations dyadiques est engendré par les permutations $\mathcal{P}_{2^j}$, $0 \leq j < v$ et est isomorphe au groupe "dyadique" $(\mathbb{F}_2^v, +)$.

Proposition 36. *Une matrice $\mathcal{M}$ carrée de taille $k = 2^v$ sur $\mathcal{L}$ est dyadique si et seulement si $\mathcal{P}_{2^j}\mathcal{M}\mathcal{P}_{2^j} = \mathcal{M}$ pour tout j, $0 \leq j < v$.*

Démonstration. La conjugaison $\mathcal{P}_{2^{v-1}}\mathcal{M}\mathcal{P}_{2^{v-1}}$ consiste à inverser les blocs $\mathcal{M}_{1,1}$ et $\mathcal{M}_{2,2}$ d'une part et les blocs $\mathcal{M}_{1,2}$ et $\mathcal{M}_{2,1}$ d'autre part. L'égalité $\mathcal{P}_{2^{v-1}}\mathcal{M}\mathcal{P}_{2^{v-1}} = \mathcal{M}$ correspond au fait que $\mathcal{M}$ est 2-blocs dyadique.

De la même manière, la conjugaison $\mathcal{P}_{2^{v-2}}\mathcal{M}\mathcal{P}_{2^{v-2}}$ préserve les sous-blocs de taille 2 et l'égalité $\mathcal{P}_{2^{v-1}}\mathcal{M}\mathcal{P}_{2^{v-1}} = \mathcal{M}$ correspond au fait que les matrices $\mathcal{M}_{1,1}$, $\mathcal{M}_{2,2}$, $\mathcal{M}_{1,2}$ et $\mathcal{M}_{2,1}$ sont 2-blocs dyadiques.

La démonstration se fait ensuite par récurrence sur i variant de $v-2$ à 0. □

Les matrices dyadiques de permutation étant involutives, la condition de la proposition est équivalente à $\mathcal{P}_{2^j}\mathcal{M} = \mathcal{M}\mathcal{P}_{2^j}$. D'autre part, les matrices $\mathcal{P}_{2^j}$ engendrant le groupe des permutations dyadiques, cette condition est encore équivalente au fait que $\mathcal{M}$ commute avec toutes les matrices de permutation dyadiques.

On note par $\mathfrak{D}_k$ l'ensemble des matrices dyadiques de taille k sur $\mathcal{L}$. Le théorème suivant est l'équivalent du théorème 23 dans le cas circulant.

Théorème 24.

1. *L'ensemble $\mathfrak{D}_k$ est le sous-$\mathcal{L}$-module de $\mathcal{L}^k$ engendré par les matrice $\mathcal{P}_i$, $0 \leq i < k$. C'est un module de rang k.*
2. *$(\mathfrak{D}_k, +, \times)$ (où $\times$ est la multiplication des matrices) est un sous-anneau de l'anneau des matrices $k \times k$ à coefficients dans $\mathcal{L}$. En particulier, si $\mathcal{M} \in \mathfrak{D}_k$ est inversible, alors $\mathcal{M}^{-1}$ est dyadique.*
3. *Si les coefficients de deux matrices dyadiques $\mathcal{M}$ et $\mathcal{M}'$ commutent, alors $\mathcal{M}\mathcal{M}' = \mathcal{M}'\mathcal{M}$.*

Démonstration.

1. La vérification est similaire à celle du théorème 23.
2. On a $\begin{pmatrix} A & B \\ B & A \end{pmatrix}\begin{pmatrix} C & D \\ D & C \end{pmatrix} = \begin{pmatrix} AC+BD & AD+BC \\ BC+AD & BD+AC \end{pmatrix}$. Le produit de deux matrices 2-blocs dyadiques est 2-blocs dyadique. Le résultat s'étend par induction au produit de deux matrices dyadiques.
   Si $\mathcal{M}$ est dyadique et inversible, la démonstration du fait que $\mathcal{M}^{-1}$ est dyadique est la même que celle du théorème 23.
3. la démonstration est la même, que celle du théorème 23.

□

Corollaire 6. *Soit $\mathcal{M}$ une matrice dyadique sur un anneau commutatif $\mathcal{A}$ de caractéristique 2, tel que $\mathcal{M} = dyad(a_0, \ldots, a_{k-1})$. Alors :*

$$\mathcal{M}^2 = \lambda \mathcal{I}_k, \text{ avec } \lambda = \sum_{i=0}^{k-1} a_i^2$$

Démonstration. La démonstration se fait par induction sur la valeur de k.

Pour $k = 2$, $\mathcal{M} = \begin{pmatrix} a_0 & a_1 \\ a_1 & a_0 \end{pmatrix}$ et alors $\mathcal{M}^2 = \begin{pmatrix} a_0^2 + a_1^2 & 0 \\ 0 & a_0^2 + a_1^2 \end{pmatrix}$.
Pour $k \geq 2$, le calcule se fait de la même manière, en employant le fait que $\mathcal{A}$ est commutative et que sa caractéristique est égale à 2. □

Á chaque entier $i \in [0; 2^v - 1]$, on associe sa décomposition binaire $\overline{i} \in \mathbb{F}_2^v$. Par exemple pour $v = 3$, $\overline{3} = (1, 1, 0)$.

Pour i et j dans $\mathbb{F}_2^v$, on note par $\overline{i} \oplus \overline{j} = \overline{i \oplus j}$ le ou-exclusif bit à bit. Par exemple $\overline{3} \oplus \overline{2} = \overline{1}$.

Proposition 37. *Si $\mathcal{M} = dyad(M_0)$, est une matrice dyadique de première ligne (ou colonne) $M_0 = (a_0, \ldots, a_{k-1})$. Alors la i-ème ligne (ou colonne) de $\mathcal{M}$ est $M_i = M_0 P_i = (a_{\overline{0 \oplus i}}, \ldots, a_{\overline{(k-1) \oplus i}})$.*

En outre pour $i, j \in [0; k-1]$, et $j \in [0; v-1]$, on a $\mathcal{P}_i \mathcal{P}_j = \mathcal{P}_{\overline{i \oplus j}}$.

Démonstration. Par définition, la première ligne de $\mathcal{P}_i$ est e_i, et puisque $\mathcal{M}$ est une matrice dyadique, alors selon le lemme 36, $\mathcal{P}_i \mathcal{M} = \mathcal{M} \mathcal{P}_i$.

La première ligne de $\mathcal{P}_i \mathcal{M}$ est $\mathcal{M}_i$, et la première ligne de $\mathcal{M}\mathcal{P}_i$ est $\mathcal{M}_0 \mathcal{P}_i$, on en déduit $\mathcal{M}_i = \mathcal{M}_0 \mathcal{P}_i$.

On commence par montrer que $\mathcal{M}_0 \mathcal{P}_i = (a_{0 \oplus i}, a_{1 \oplus i}, ..., a_{(k-1) \oplus i})$ pour $i = 2^j$, $j \in [0; v-1]$

Pour $i = 2^0 = 1$, on a

$$\mathcal{P}_1 = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

Alors :

$$\mathcal{M}_0\mathcal{P}_1 = (a_1, a_0, a_3, a_2, ..., a_{k-1}, a_{k-2}) = (a_{0\oplus 1}, a_{1\oplus 1}, ..., a_{(k-1)\oplus 1})$$

Pour $i = 2$, on a :

$$\mathcal{P}_2 = \begin{pmatrix} 0_2 & I_2 & & & & & \\ I_2 & 0_2 & & & & & \\ & & 0_2 & I_2 & & & \\ & & I_2 & 0_2 & & & \\ & & & & \ddots & & \\ & & & & & 0_2 & I_2 \\ & & & & & I_2 & 0_2 \end{pmatrix}.$$

En effet :

$$\mathcal{M}_0\mathcal{P}_2 = (a_2, a_3, a_0, a_1, ..., a_{k-2}, a_{k-1}, a_{k-4}, a_{k-3}) = (a_{0\oplus 2}, a_{1\oplus 2}, ..., a_{((k-1)\oplus 2)}).$$

Et ainsi de suite pour $i = 2^u$ à $i = 2^v$:

$$\mathcal{P}_{2^{v-1}} = \begin{pmatrix} 0_{2^{v-1}} & I_{2^{v-1}} \\ I_{2^{v-1}} & 0_{2^{v-1}} \end{pmatrix}$$

et

$$\mathcal{M}_0\mathcal{P}_{2^{v-1}} = (a_{2^{v-2}}, ..., a_{k-1}, a_0, ..., a_{2^{v-2}-1}) = (a_{0\oplus 2^{v-1}}, a_{1\oplus 2^{v-1}}, ..., a_{((k-1)\oplus 2^{v-1})}).$$

En particulier, si $\mathcal{M} = \mathcal{P}_i = dyad(e_l)$ pour un certain l, alors on peut conclure que $e_l\mathcal{P}_{2^j} = e_{l\oplus 2^j}$.

Utilisons la décomposition binaire de $i = \sum_{l=0}^{v-1} i_l 2^l$, on déduit que $e_j\mathcal{P} = e_{i\oplus j}$.

Puisque le produit de deux matrices de permutation dyadiques, est une matrice de permutation dyadique, alors il existe un entier l tel que $\mathcal{P}_i\mathcal{P}_j = \mathcal{P}_l$, cet entier est entièrement déterminé par la première ligne du produit, qui est $e_l = e_{i+j}$, c'est-à-dire $\mathcal{P}_i\mathcal{P}_j = \mathcal{P}_{\overline{i\oplus j}}$.
Pour conclure cette démonstration, on peut remarquer que $\mathcal{M} = \sum_{i=0}^{k-1} a_j\mathcal{P}_j$. □

8.3.3 Produit de Kronecker et matrices dyadiques

Il existe un lien fort entre les matrices dyadiques et le produit de Kronecker. En particulier, les matrices de permutation dyadiques peuvent être construites récursivement à l'aide du produit de Kronecker des matrices. On rappelle que si $\mathcal{M} = (a_{i,j})$ et $\mathcal{N}$ sont deux matrices, le produit de Kronecker (ou produit tensoriel) est défini par $\mathcal{M} \otimes \mathcal{N} = (a_{i,j}\mathcal{N})$.

Par exemple, si $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, alors $I_2 \otimes J_2 = \begin{pmatrix} J_2 & 0 \\ 0 & J_2 \end{pmatrix}$

Lemme 13. *Si $\mathcal{M}$ et $\mathcal{N}$ sont deux matrices dyadiques de taille respective $k' = 2^{v'}$ et $k'' = 2^{v''}$, alors $\mathcal{M} \otimes \mathcal{N}$ est une matrice dyadique de taille $k = k'k''$.*

Démonstration. Par récurrence sur v'. Pour $v' = 1$, si $\mathcal{M} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$, alors le produit $\mathcal{M} \otimes \mathcal{N} = \begin{pmatrix} a_1 N & a_2 N \\ a_2 N & a_1 N \end{pmatrix}$ est clairement dyadique.

Dans le cas général, si on décompose $\mathcal{M}$ en sous-blocs de taille $k'/2$, en utilisant les notations du paragraphe 8.3.1, on obtient

$\mathcal{M} \otimes \mathcal{N} = \begin{pmatrix} \mathcal{M}_{1,1}\mathcal{N} & \mathcal{M}_{1,2}\mathcal{N} \\ \mathcal{M}_{1,2}\mathcal{N} & \mathcal{M}_{1,1}\mathcal{N} \end{pmatrix}$, ce qui permet de montrer par récurrence directe que la matrice $\mathcal{M} \otimes \mathcal{N}$ est dyadique. □

On peut construire toutes les matrices de permutation dyadiques par produits tensoriels successifs des deux matrices I_2 et J_2 précédemment. Supposons que l'on regarde la matrice de permutation $\mathcal{P}_i$ pour $k = 2^v$. Pour $0 \leq i < k$, on peut associer à i le v-uplet binaire de sa décomposition en base 2 : $\overline{i} = (i_{v-1}, ..., i_0)$, $i_j \in \{0, 1\}$ et $i = \sum_{j=0}^{v-1} i_j 2^j$.

Proposition 38. *Si $\mathcal{P}_i$ est la matrice de permutation dyadique de taille $k = 2^v$ définie précédemment, alors $\mathcal{P}_i = J_2^{i_{v-1}} \otimes J_2^{i_{v-2}} \otimes \ldots \otimes J_2^{i_0}$.*

Démonstration. La démonstration se fait par récurrence sur v :

Pour $v = 1$, il s'agit juste de la notation $J_2^0 = I_2$.

Supposons que c'est vrai pour $v - 1$, et montrons le résultat pour v :

Pour $\overline{i} = (i_{v-1}, ..., i_0)$, on pose $i' = i \div 2 \in [0, \ldots, 2^{v-1}[$. La permutation $\mathcal{P}_{i'}$ est de taille $k/2$ et on a $\overline{u'} = (i_{v-1}, ..., i_1)$. Par hypothèse de récurrence, on a $\mathcal{P}_{i'} = J_2^{i_{v-1}} \otimes J_2^{i_{v-2}} \otimes \ldots \otimes J_2^{i_1}$.

Il suffit alors de vérifier que, pour $i_0 = 0$, on a $\mathcal{P}_i = dyad(e_i) = \mathcal{P}_{i'} \otimes I_2$, et pour $i_0 = 1$, on a $\mathcal{P}_i = dyad(e_i) = \mathcal{P}_{i'} \otimes J_2$.

□

Par exemple pour $v = 3$, on a : $\mathcal{P}_1 = I_2 \otimes I_2 \otimes J_2 = \begin{pmatrix} J_2 & 0 & 0 & 0 \\ 0 & J_2 & 0 & 0 \\ 0 & 0 & J_2 & 0 \\ 0 & 0 & 0 & J_2 \end{pmatrix}$

et $\mathcal{P}_4 = J_2 \otimes I_2 \otimes I_2 = \begin{pmatrix} 0 & I_4 \\ I_4 & 0 \end{pmatrix}$.

Nous allons voir maintenant que le produit de Kronecker ne permet pas de construire toutes les matrices dyadiques.

Proposition 39. *L'ensemble des matrices dyadiques de taille k de la forme $\bigotimes_{j=0}^{v-1} D_j^{(2)}$, où les matrices $D_j^{(2)}$ sont dyadiques de taille 2, n'est pas égal à l'ensemble $\mathfrak{D}_k$ de toutes les matrices dyadiques de taille k.*

Démonstration. Il suffit de compter chacun de ses ensembles : si $N = \#\mathcal{L}$, il y a N^2 matrices dyadiques de taille 2. D'autre part, $\mathfrak{D}_k$ est un $\mathcal{L}$-module de rang k, il a donc N^k éléments. Le nombre de matrices dyadiques de taille k obtenue par produit tensoriel est au plus N^{2v}. □

La proposition suivante prouve que le produit de Kronecker n'est pas une bonne approche pour construire des matrices MDS.

Proposition 40. *Soit $\mathcal{M}$ une matrice de $\mathfrak{D}_v$ tel que $\mathcal{M} = U \otimes V$ avec $U \in \mathfrak{D}_1$ et $V \in \mathfrak{D}_{v-1}$, alors $\mathcal{M}$ n'est pas une matrice MDS.*

Démonstration. Puisque on a le droit de multiplier $\mathcal{M}$ par un élément inversible de $\mathcal{L}$, on peut supposer que $U = \begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix}$ pour $(1, u) \in \mathcal{L}^2$, et $V = \begin{pmatrix} I_{2^{v-2}} & W \\ W & I_{2^{v-2}} \end{pmatrix}$, pour $(W, I_{2^{v-2}}) \in (\mathfrak{D}_{v-2})^2$.

Le produit de Kronecker nous donne :

$$\mathcal{M} = U \times V = \begin{pmatrix} I_{2^{v-2}} & W & uI_{2^{v-2}} & uW \\ W & I_{2^{v-2}} & uW & uI_{2^{v-2}} \\ uI_{2^{v-2}} & uW & I_{2^{v-2}} & W \\ uW & uI_{2^{v-2}} & W & I_{2^{v-2}} \end{pmatrix}$$

On remarque très facilement, que la sous-matrice :

$$\begin{pmatrix} uW & uI_{2^{v-2}} \\ W & I_{2^{v-2}} \end{pmatrix}$$

n'est pas inversible, d'où le fait que $\mathcal{M}$ n'est pas MDS.

□

8.4 Équivalence des matrices structurées

Le but de cette section est d'étudier l'équivalence entre les matrices MDS structurées, afin d'optimiser la recherche exhaustive de la section 8.6.2 des matrices MDS.

L'équivalence des matrices MDS a été étudiée à la section 7.1.4. En particulier si une matrice est MDS, les matrices équivalentes sont aussi MDS.

Si de plus une matrice MDS $\mathcal{M}$ est structurée, il est intéressant pour une classification de ce type de matrices, de déterminer parmi les matrices équivalentes à $\mathcal{M}$ celles qui ont la même structure. Pour simplifier l'approche, nous allons étudier séparément l'équivalence par permutation et l'équivalence par multiplication scalaire.

8.4.1 Équivalence par permutation

En utilisant le lemme 5, on sait que pour toutes permutations P et P', si $\mathcal{M}$ est une matrice MDS, alors $P\mathcal{M}P'$ est MDS. D'après le théorème 23, le produit de deux matrices circulantes est une matrice circulante et l'inverse d'une matrice circulante inversible est matrice circulante.

On en déduit la proposition suivante :

Proposition 41. *Soit $\mathcal{M}$ une matrice MDS circulante. Soit P une matrice de permutation. La matrice $P\mathcal{M}$ (ou encore $\mathcal{M}P$) est MDS circulante si et seulement si $P = S^i$ est une matrice de permutation circulante.*

Démonstration. La matrice $\mathcal{M}$ est MDS, donc inversible. Si $P\mathcal{M}$ est circulante, il en est de même pour $P = P\mathcal{M}\mathcal{M}^{-1}$. Les seules matrices de permutation circulantes étant les multiples de S, le résultat est démontré. □

De manière analogue, à partir du théorème 24, on obtient la proposition

Proposition 42. *Soit $\mathcal{M}$ une matrice MDS dyadique. Soit P une matrice de permutation. La matrice $P\mathcal{M}$ (ou encore $\mathcal{M}P$) est MDS dyadique si et seulement si $P = \mathcal{P}_i$ est une matrice de permutation dyadique.*

On peut remarquer que, si $\mathcal{M}$ est circulante, alors $S^i\mathcal{M} = \mathcal{M}S^i$. De même, si $\mathcal{M}$ est dyadique, alors $\mathcal{P}_i\mathcal{M} = \mathcal{M}\mathcal{P}_i$. A partir d'une matrice $\mathcal{M}$ MDS structurée, on peut alors construire k matrices structurées équivalentes par permutations en multipliant cette matrice soit par S^i dans le cas circulant, soit par $\mathcal{P}_i$ dans le cas dyadique.

8.4.2 Équivalence par multiplication scalaire

En suivant les résultats de la proposition 35 et de la définition 40, il faut déterminer quelles sont les matrices diagonales D_1 et D_2 inversibles à coefficients dans $\mathcal{L}$ telles que, si $\mathcal{M}$ est circulante (ou dyadique), alors $D_1\mathcal{M}D_2$ est circulante (ou dyadique).

Supposons que les matrices diagonales D_1 et D_2 soient des matrices scalaires, c'est-à-dire $D_1 = \varphi_1\mathcal{I}_k$ et $D_2 = \varphi_2\mathcal{I}_k$, avec $\varphi_i \in GL(m, 2)$.

Il est immédiat de vérifier que, si $\mathcal{M}$ est circulante (resp. dyadique), alors $D_1\mathcal{M}D_2$ est circulante (respectivement dyadique). En particulier, si $\mathcal{M} = (m_{i,j})$, alors $D_1\mathcal{M}D_2 = (\varphi_1 m_{i,j}\varphi_2)$.

Dans le cadre d'une recherche exhaustive sur les matrices MDS structurées, on peut faire une première normalisation consistant à fixer les matrices, en particulier en fixant le premier coefficient de $\mathcal{M}$ à la valeur $m_{1,1} = Id = 1_{\mathcal{L}}$. On dira dans ce cas que $\mathcal{M}$ est une matrice MDS normalisée.

Lemme 14. *Soient $\mathcal{M}$ et $\mathcal{M}'$ deux matrices MDS circulantes ou dyadiques normalisées. S'il existe deux matrices diagonales D_1 et D_2 telles que $\mathcal{M}' = D_1\mathcal{M}D_2$, alors $D_2 = D_1^{-1}$.*

Démonstration. On note φ_i etφ'_i les éléments des diagonales respectives de D_1 et D_2. Si $\mathcal{M}$ et $\mathcal{M}'$ sont deux matrices circulantes ou dyadiques, et si de plus elle sont normalisées, alors $m_{i,i} = m'_{i,i} = 1$ pour tout i. En particulier, cela implique que $\varphi_i\varphi'_i = 1$ pour tout i, ce qui démontre le Lemme. □

Il est facile de vérifier que cette condition n'est pas suffisante. En effet, si on considère le cas dyadique, on obtient par exemple que l'on doit aussi avoir la condition suivante : $\varphi_2 m_2\varphi_1^{-1} = \varphi_1 m_2\varphi_2^{-1}$ (avec la notation

$\mathcal{M} = dyad(m_1, m_2, ...)$). Ceci signifie que $\varphi_1^{-1}\varphi_2$ doit commuter avec m_2. En conséquence, il est possible de trouver des cas particuliers d'équivalence, mais impossible de trouver une équivalence qui préserve de manière générale les matrices structurées, à l'exception des matrices scalaire : $D_1 = \varphi I_k$ et $D_2 = D_1^{-1}$. Cette condition conduit à une équivalence scalaire limitée dans le cas structuré.

Définition 45. *Deux matrices structurées normalisées* $\mathcal{M} = (m_{i,j})$ *et* $\mathcal{M}' = (m'_{i,j})$ *sont scalairement équivalentes si, pour tout* i *et* j *dans* $[1, \ldots, k]$*, il existe* $\varphi \in GL(m, 2)$ *tel que* $m'_{i,j} = \varphi m_{i,j} \varphi^{-1}$.

8.5 Méthodologie de recherche exhaustive

8.5.1 Vérification de la propriété MDS

Une des difficultés majeures lors de la recherche exhaustive des matrices MDS est l'algorithme de test qui détermine si une matrice de taille $k \times k$ dans $\mathcal{L}$ est MDS.

La structure de $\mathcal{L}$, qui est un anneau non commutatif, ne nous permet pas de calculer les sous-déterminants des matrices à tester. Ce point est cependant un faux problème, puisqu'on a vu à la proposition 32 qu'il suffit de faire les tests sur les déterminants par blocs en utilisant la matrice M, image binaire de $\mathcal{M}$.

La difficulté réside dans le nombre de sous-déterminants par blocs à calculer pour déterminer si une matrice est MDS.

En lien avec les applications cryptographiques, et du fait que la taille des matrices dyadiques est forcément une puissance de 2, nous concentrerons nos efforts sur les longueurs (par blocs) de la forme $k = 2^v$. Un simple test pour démontrer qu'une matrice de taille $k = 8$ est MDS, est relativement coûteux et ne peut être utilisé que ponctuellement. La taille m des blocs n'intervient que linéairement dans ce test et n'est pas l'obstacle principal.

La construction des matrices MDS, est liée à la conjoncture des codes MDS, telle que, hors cas particuliers, la longueur maximale n d'un code MDS sur un alphabet de taille q est $n = q + 1$. Ainsi pour un code MDS sur l'alphabet $\mathbb{F}_2^m$, et puisque la longueur de nos codes $s = 2k$ est paire, alors, si on fixe la taille des blocs m, la taille maximale d'une matrice MDS est $k = 2^{m-1}$, ou bien, si on fixe une taille de matrice $k = 2^v$, la taille maximale de chaque bloc est $m = v + 1$.

Les propriétés de symétrie dans les matrices dyadiques et circulantes nous permettent de réduire le nombre de sous-déterminants à calculer.

Le tableau ci-dessous donne le nombre de déterminants à calculer lorsque $k = 4$, selon que l'on considère une matrice quelconque, une matrice circulante ou une matrice dyadique. La taille des déterminants correspond à la taille en image binaire et est donc un multiple de m.

taille des déterminants	m	$2m$	$3m$	$4m$
matrice quelconque	16	36	16	1
matrice circulante	4	12	8	1
matrice dyadique	4	12	4	1

Ces nombres de déterminants correspondent au cas où la matrice M est MDS par blocs. Dans le cas général, si la matrice n'est pas MDS, un des sous-déterminants est nul et le test s'arrête très rapidement (en général, après au plus 3 tests de déterminants de taille $2m$).

8.5.2 Méthodologie

Les recherches exhaustives ont été faites en utilisant le système de calcul formel **Magma**. Dans le cas de la recherche de matrices à coefficients dans le corps fin $\mathbb{F}_{2^m}$, nous avons utilisé directement les outils de **Magma** [12]. Dans le cas des matrices sur l'anneau $\mathcal{L}$, nous avons utilisé les matrices $km \times km$ images binaires, et avons construit ces matrices à partir des matrices du groupe linéaire $GL(m, 2)$ directement disponibles dans **Magma**.

La normalisation et la conjugaison des coefficients par une matrice $M_\varphi \in GL(m, 2)$ a été systématiquement utilisée.

Un autre point important est que, si une matrice structurée est MDS, certains de ses sous-blocs sont structurés et MDS. La classification des matrices structurées de taille k peut prendre en compte de manière efficace les résultats obtenus pour la taille $k/2$.

Par exemple, si M est une matrice dyadique MDS et $\begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{1,2} & M_{1,1} \end{pmatrix}$ sa décomposition en blocs de taille $k/2$, les matrices $M_{1,1}$ et $M_{1,2}$ sont elles-même des matrices dyadiques MDS.

8.5.3 Matrices MDS structurées de taille $k = 2$

Pour les matrices de taille $k = 2$, les deux notions de matrices dyadiques et de matrices circulantes coïncident.

Pour caractériser les matrices MDS dyadiques par blocs M de taille $k = 2$, on suppose que M est normalisée, c'est-à-dire est de la forme

$$M = \begin{pmatrix} Id & M_\varphi \\ M_\varphi & Id \end{pmatrix}$$

avec $M_\varphi \in GL(m, 2)$.

La matrice $\mathcal{M}$ associée est $\mathcal{M} = \begin{pmatrix} 1 & \varphi \\ \varphi & 1 \end{pmatrix}$. On peut remarquer que les coefficients de $\mathcal{M}$ commutent.

La matrice $\mathcal{M}$ est MDS si et seulement si $det_{\mathcal{L}}(\mathcal{M})$ est non nul. La matrice $m \times m$ image binaire de $det_{\mathcal{L}}(\mathcal{M})$, est $Id - M_\varphi^2 = (Id - M_\varphi)^2$.

On a ainsi démontré le résultat suivant :

Proposition 43. *Une matrice dyadique $\mathcal{M}$ de la forme $\mathcal{M} = \begin{pmatrix} 1 & \varphi \\ \varphi & 1 \end{pmatrix}$ est MDS, si et seulement si le polynôme caractéristique de φ ne s'annule pas en 0 et 1.*

Démonstration. En effet, 0 ne peut être racine du polynôme caractéristique car φ est inversible, de plus 1 n'est pas racine de ce polynôme car $(Id - M_\varphi)^2 \neq 0$. □

Les matrices 2×2 dyadiques s'obtiennent à partir de celles décrites dans cette proposition par multiplication scalaire par un élément de $GL(m, 2)$.

Dans le cadre d'une recherche exhaustive par exemple pour $k = 4$, on construit d'abord la liste des bons candidats de taille 2 pour limiter cette recherche aux éléments susceptibles de conduire à une matrice MDS.

8.6 Recherche exhaustive

Cette section présente un certain nombre de résultats de recherche exhaustive sur les matrices MDS dyadiques et circulantes. Pour permettre les comparaisons et respecter les valeurs habituellement utilisées en cryptographie, nous nous sommes limités aux valeurs de 4 et 8 pour m ainsi que pour k.

8.6.1 Cas des corps finis

Dans la littérature, la plupart des matrices MDS structurées utilisées sont dérivés à partir de la structure des corps finis $\mathbb{F}_{2^m}$. Ainsi les applications ϕ_i de l'anneau des endomorphismes $\mathcal{L}$ correspondent aux multiplications dans ces corps finis.

Dans ce cas les matrices MDS structurées normalisées de taille $k = 2$ sont celles de la forme $\begin{pmatrix} 1 & \beta \\ \beta & 1 \end{pmatrix}$ avec $\beta \in \mathbb{F}_{2^m}$, $\beta \neq 0$ et $\beta \neq 1$, ce qui implique que le nombre de ces matrices MDS est $2^m - 2$.

Dans le cas des matrices MDS sur un corps fini, on peut introduire un autre invariant pour la distance de Hamming. On définit l'application de Frobenius F de $\mathbb{F}_{2^m}$ dans lui-même par $F(a) = a^2$.

Soit $\mathbf{M}$ une matrice à coefficients dans $\mathbb{F}_{2^m}$. On note par $F(\mathbf{M})$ la matrice obtenue en appliquant l'endomorphisme F à chaque coefficient de $\mathbf{M}$. On sait que F est bijective alors c'est un automorphisme de corps, ainsi pour une matrice carrée $\mathbf{M}$, on a $det(F(\mathbf{M})) = F(det(\mathbf{M}))$. En conséquence, si $\mathbf{M}$ est MDS, alors $F(\mathbf{M})$ est aussi MDS.

Afin de déterminer le nombre de matrices normalisées structurées de taille 4×4 (notamment le cas des matrices dyadiques et circulaires), il suffit de calculer le nombre de matrices ayant la première ligne de la forme $(1, b, c, d)$, tel que b est choisi dans un ensemble de représentants des classes de conjugaison par F (sauf les classes 0 et 1), et c et d sont dans $\mathbb{F}_{2^m}$.

Dans le cas des matrices dyadiques, en appliquant la permutation $\mathcal{P}_1$ à la matrice MDS normalisée de première ligne $(1, b, c, d)$, on obtient la matrice MDS dyadique de première ligne $(b, 1, d, c)$. Après normalisation, on obtient une matrice MDS de première ligne $(1, b^{-1}, b^{-1}d, b^{-1}c)$, ce qui implique en particulier que le nombre de solutions pour un b fixe est le même nombre de solutions pour b^{-1}. Ainsi on peut restreindre la valeur de b à un représentant par réunion des classes de b et b^{-1}.

Le tableau ci-dessous donne le nombre de matrices MDS structurées et normalisées, dérivées du corps fini $\mathbb{F}_{2^m}$ pour $k = 4$, obtenu par une recherche exhaustive en utilisant les remarques données ci-dessus :

m	4	5	6	7	8
Dyadique	1512	21000	212040	1890504	15937992
Circulante	1104	18720	201306	1844640	15747984

TABLE 8.1 – Matrices MDS dyadiques et circulantes sur $\mathbb{F}_{2^m}$ pour $k = 4$.

On peut remarquer que, pour les petites valeurs de m, il y a plus de matrices MDS dyadiques que circulantes, par contre, cette propriété semble disparaître lorsque m grandit.

On a observé que, dans le cas des matrices dyadiques, et on a vérifié que, quelque soit l'élément $b \notin \{0, 1\}$ choisi, on a le même nombre de solutions de la forme $dyad(1, b, c, d)$. D'autre part, le nombre total de matrices MDS normalisées dyadiques est $(2^m - 2)(2^m - 4)(2^m - 7)$ pour les valeurs de m étudiées.

Malheureusement, nous n'avons pas réussi à démontrer ce résultat dans le cas général, il reste donc pour le moment une conjoncture.

8.6.2 Recherche exhaustive pour $m = 4$ et $k = 4$

Dans cette section, on s'intéresse aux matrices MDS structurées pour $m = 4$ et $k = 4$. Ce sont donc les matrices 4×4 à coefficients dans $GL(4, 2)$.

Cas dyadique

On considère une matrice dyadique $\mathcal{M} = dyad(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, avec $\varphi_i \in GL(4, 2)$. La recherche exhaustive sur $GL(4, 2)^4$ semble difficile, vu le coût du test MDS et du nombre d'éléments à tester (environ $2^{14.3}$).

On normalise alors $\mathcal{M}$ en fixant $\varphi_1 = 1_{\mathcal{L}}$.

On a alors

$$\mathcal{M} = \begin{pmatrix} 1 & \varphi_2 & \varphi_3 & \varphi_4 \\ \varphi_2 & 1 & \varphi_4 & \varphi_3 \\ \varphi_3 & \varphi_4 & 1 & \varphi_2 \\ \varphi_4 & \varphi_3 & \varphi_2 & 1 \end{pmatrix}.$$

Si $\mathcal{M}$ est MDS, cela implique que $dyad(1, \varphi_2)$, $dyad(1, \varphi_3)$, $dyad(1, \varphi_4)$, $dyad(\varphi_2, \varphi_3)$ et $dyad(\varphi_3, \varphi_4)$ sont aussi MDS.

Nous allons utiliser la conjugaison $\psi\mathcal{M}\psi^{-1}$ pour explorer les candidats potentiels pour l'endomorphisme φ_3. En utilisant la proposition 43, les seuls candidats pour être le polynôme caractéristique de φ_3 sont X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$ ou $X^4+X^2+1=(X^2+X+1)^2$.

Nous allons faire la recherche exhaustive sur la représentation binaire des endomorphismes. A conjugaison près, on peut alors réduire la recherche de M_{φ_3} aux 5 matrices suivantes :

$$M_1=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{pmatrix},\ M_2=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&1\end{pmatrix},\ M_3=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&1&1\end{pmatrix},$$
$$M_4=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&1&0\end{pmatrix}\text{ et }M_5=\begin{pmatrix}0&1&0&0\\1&1&0&0\\0&0&0&1\\0&0&1&1\end{pmatrix}.$$

Considérons maintenant les deux conditions "$dyad(1,\varphi_2)$ et $dyad(1,\varphi_4)$ sont MDS".

Pour $m=4$ il existe 5824 éléments de $GL(4,2)$ qui donnent des matrices MDS normalisées dyadiques de taille 2×2. Les deux isomorphismes φ_2 et φ_4 doivent être choisis dans cette liste.

De plus, les deux conditions "$dyad(\varphi_2,\varphi_3)$ et $dyad(\varphi_3,\varphi_4)$ sont MDS", sont équivalentes au fait que $dyad(1,\varphi_3^{-1}\varphi_2)$ et $dyad(1,\varphi_3^{-1}\varphi_4)$ sont MDS.

Si on a fixé l'endomorphisme φ_3, pour chacun des 5824 candidats pour φ_2 (ou φ_4), on teste alors si $(\varphi_3^{-1}\varphi_2)$ est dans la liste afin d'obtenir une liste plus réduite.

Voici le principe de l'algorithme qui nous a permis d'obtenir les résultats du tableau ci-après.

1. Construire la liste L des 5824 candidats correspondants aux matrices MDS dyadiques normalisées de taille 2.
2. pour $i=1$ à 5, $\varphi_3:=M_i$.
3. construire la liste $L'\subset L$ des éléments $\varphi\in L$ tels que $\varphi_3^{-1}\varphi\in L$.
4. faire la recherche exhaustive des matrices MDS obtenue en prenant $\varphi_2\in L'$ et $\varphi_4\in L'$.
5. Multiplier le nombre des solutions par le nombre des conjugués de φ_3, dans $GL(4,2)$.

Le nombre des conjugués dans $GL(4,2)$ de M_1, M_2, M_3 est $\#GL(4,2)/15=1344$, le nombre des conjugués de M_4 est $\#GL(4,2)/12=1680$ et le nombre des conjugués de M_5 est $\#GL(4,2)/180=112$.

φ_3	M_1	M_2	M_3	M_4	M_5
Solutions normalisées	110	150	140	92	984
Solutions conjuguées	147840	201600	188160	154560	110208

On obtient un nombre total de 802368 matrices MDS dyadiques normalisées sur $GL(4,2)$. Ce nombre est plus grand que celui de matrices obtenues à partir de la conjugaison des matrices dérivées du corps fini $\mathbb{F}_{2^4}$, qui est 1512. Par exemple, l'ordre de la matrice M_4 est 6, qui ne divise pas l'ordre du groupe multiplicatif de $\mathbb{F}_{16}$ qui est 15. Cette dernière n'est donc pas équivalente à une matrice de multiplication dans le corps fini.

Cas circulant

Les méthodes appliquées dans le cas dyadique peuvent être modifiées dans le cas circulant. On considère donc une matrice circulante normalisée $\mathcal{M} = circ(1, \varphi_2, \varphi_3, \varphi_4)$.

On a donc

$$\mathcal{M} = \begin{pmatrix} 1 & \varphi_2 & \varphi_3 & \varphi_4 \\ \varphi_4 & 1 & \varphi_2 & \varphi_3 \\ \varphi_3 & \varphi_4 & 1 & \varphi_2 \\ \varphi_2 & \varphi_3 & \varphi_4 & 1 \end{pmatrix}$$

Si $\mathcal{M}$ est une matrice MDS alors les matrices $circ(1, \varphi_3)$, $circ(\varphi_i, \varphi_j)$ et $circ(\varphi_2, \varphi_4)$ sont MDS. On pose $\varphi_4' = \varphi_2^{-1}\varphi_4$, il est facile alors de vérifier que $circ(1, \varphi_4')$ est MDS, en revanche on n'a à priori pas de contraintes sur φ_2.

On va donc procéder à une recherche exhaustive sur φ_2 avant d'utiliser des techniques similaires au cas dyadique.

1. Construire la liste L des 5824 candidats correspondants aux matrices MDS circulantes normalisées de taille 2.
2. Pour $i = 1$ à 5, $\varphi_3 = M_i$.
3. Pour chaque φ_2 dans $GL(4,2)$ faire.
4. Pour $\varphi_4' \in L$, faire le test MDS sur $circ(1, \varphi_2, \varphi_3, \varphi_2\varphi_4')$.
5. Multiplier le nombre de solutions normalisées par le nombre de conjuguées de $\varphi_3 = M_i$ dans $GL(4,2)$.

Les résultats obtenus sont les suivants :

φ_3	M_1	M_2	M_3	M_4	M_5
Solutions normalisées	1106	1106	1314	1088	27601
Solution conjuguées	1486464	1486464	1766016	1827840	309120

On obtient un nombre total de 6875904 matrices MDS circulantes normalisées sur $GL(4,2)$. Ce nombre est bien plus grand que le nombre obtenu dans le cas dyadique, et aussi plus grand que celui des matrices obtenues à partir de la conjugaison des matrices dérivées du corps fini $\mathbb{F}_{2^4}$.

Conclusion

Il est intéressant de remarquer que, si on recherche le nombre de matrices MDS structurées à coefficients dans $\mathcal{L}$, le nombre de matrices circulantes semble bien plus élevé (environ 8 fois plus dans le cas $m = 4$ et $k = 4$) que celui des matrices dyadiques.

Ce résultat est l'inverse de ce qui a été obtenu lorsqu'on s'est contenté d'explorer les matrices à coefficients dans le corps fini $\mathbb{F}_{2^4}$.

Nous n'avons pas trouvé d'explication à ce phénomène, si ce n'est que les contraintes sur φ_2 sont relâchées dans le cas circulant par rapport au cas dyadique.

8.7 Optimisation pour la cryptographie

Dans cette section, nous cherchons à construire des matrices de diffusion MDS qui soient efficaces pour les implémentations matérielle et logicielle.

En pratique, on utilise seulement trois types de matrices MDS pour la diffusion : les matrices circulantes, les matrices dyadiques, et la méthode dite "récursive" qui permet d'obtenir une matrice MDS de taille k en itérant k fois une matrice compagnon [2, 3, 7, 37, 43, 47].

Nous ne nous intéresserons pas ici à cette dernière méthode.

En ce qui concerne les implémentations logicielle, celles-ci se font maintenant systématiquement avec des matrices circulantes ou dyadiques, mais sont ensuite implémentées en tables, qui réunissent en une seule lecture le calcul de la S-boxe et celui de la diffusion MDS. Du coup, toutes les matrices structurées ont un coût équivalent.

Ceci n'est évidemment pas le cas des implémentations matérielles, ou de certaines implémentations logicielles en environnement contraint, comme exemple des contraintes de mémoire.

8.7.1 Optimisation des implémentations contraintes

Implémentation matérielle

Dans le contexte d'une implémentation matérielle, on cherche à minimiser la taille du circuit, la consommation de courant, et la latence du circuit. Il est difficile de définir des critères généraux convenant à toutes les implémentations.

Dans le cas des matrices de diffusion, l'évaluation est en fait plus facile : une fois que l'on a fixé la taille des blocs, leurs nombres, ainsi que l'utilisation d'une matrice MDS structurée, les implémentations efficaces sont celles qui nécessitent le moins de portes XOR, afin de minimiser à la fois la taille du circuit et la consommation de courant.

Si M est une matrice binaire de taille r, on note par $w = w(M)$ son poids de Hamming, c'est-à-dire le nombre coefficients non nuls de M. Le nombre de XORs nécessaires pour appliquer la matrice M à un r-uplet binaire est alors

$w - r$. Dans la suite M sera soit de la forme M_φ, c'est-à-dire de taille $m \times m$, soit l'image binaire d'une matrice MDS $\mathcal{M}$, et donc $r = km$.

Implémentation logicielle

Dans le cadre des implémentations logicielles, la taille des mots machine est m (ou un multiple de m). Dans ce cas une matrice sous forme compagnon est un bon candidat pour cette implémentation.

On donne ci-dessous un exemple de l'implémentation de la matrice compagnon de taille 8×8 (elle agit sur des mots de taille 8) suivante :

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Soit $x = (x_0, x_1, \ldots, x_7) \in \mathbb{F}_2^8$, alors M agit sur les mots de la manière suivante : $y = (y_0, y_2, \ldots, y_7) = xM$.

On pose $a = (1, 0, 1, 1, 0, 0, 1, 1)$ le masque de la dernière ligne de M, alors $y = x_{>>1} \oplus (x_7 a)$, tel que $x_{>>1} = (0, x_0, \ldots, x_6)$, et ($x_7 a = (0, \ldots, 0)$ si $x_7 = 0$, et $x_7 a = a$ si $x_7 = 1$).

Les matrices compagnons ne peuvent être utilisées que pour les matrices de $GL(m, 2)$, on ne peut pas obtenir directement de matrices MDS avec celles-ci.

Un bon exemple de matrice de diffusion MDS, qui est efficace à la fois d'un point de vue matériel et logiciel, est la matrice MixColumns de l'AES. C'est une matrice MDS circulante, de taille $k = 4$, agissant sur des blocs de taille $m = 8$.

Elle est construite à partir du corps fini $\mathbb{F}_{2^8}$ de la manière suivante :

Soit β une racine du polynôme irréductible non-primitif $Q(X) = X^8 + X^4 + X^3 + X + 1$, la matrice MixColumns est $MC = circ(\beta, \beta + 1, 1, 1)$. On pose M_β la matrice compagnon de $Q(X)$. En logiciel, $M_{\beta+1}$ peut être calculée en appliquant M_β à X, puis On note que le poids de Hamming de la matrice MixColumns binaire de taille 32×32 est 192.

Dans la suite, nous allons essayer d'optimiser le poids de Hamming de nos matrices de diffusion MDS.

8.7.2 Un exemple optimal pour $k = 2$

Pour une taille de blocs m fixée on définit la matrice circulante de taille m dite de permutation circulaire $S = circ(0, 1, 0, ..., 0)$.

Pour $1 \leq j \leq m$ on note $E^{(j)}$ la matrice ayant des coefficients nuls excepté le coefficient correspondant à la dernière ligne et la j-ème colonne.

Le lemme suivant se vérifie directement.

Lemme 15. *Pour $1 < j \leq m$, la matrice $M^{(j)} = S + E^{(j)}$ est inversible et a pour polynôme caractéristique $q(X) = X^m + X^{j-1} + 1$.*

En utilisant ce lemme, on en déduit la proposition suivante :

Proposition 44. *Pour tout $m > 1$, pour tout j, $1 < j \leq m$, la matrice circulante (et dyadique) $M = circ(1, M^{(j)})$ est MDS. Son poids de Hamming $w(M) = 4m + 2$ est minimal par rapport aux matrices MDS par blocs de paramètre $k = 2$.*

Démonstration. La démonstration de la propriété MDS est la conséquence directe du lemme précédent et de la proposition 43. Si $M = circ(1, M_\varphi)$, le poids de Hamming de M est $2m+2w(M_\varphi)$. Si M est MDS, alors φ ne peut pas être l'identité et le poids de M_φ est au moins $m+1$, donc $w(M) \geq 4m+2$. □

Par exemple, la matrice binaire

$$M = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&1\\ 0&0&0&1&1&1&0&0\\ \hline 0&1&0&0&1&0&0&0\\ 0&0&1&0&0&1&0&0\\ 0&0&0&1&0&0&1&0\\ 1&1&0&0&0&0&0&1 \end{array}\right).$$

est une matrice de diffusion MDS, qui agit sur 2 blocs de taille 4 bits.

8.7.3 Cas dyadique pour $m = 4$ et $k = 4$

Soit $\mathcal{M} = dyad(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ avec $\varphi_i \in GL(4, 2)$, pour $1 \leq i \leq 4$. Le poids de Hamming de la matrice image binaire M est 4 fois la somme des poids de Hamming des matrices M_{φ_i}.

Pour $m = 4$, il est possible de faire une recherche exhaustive pour obtenir les matrices de petit poids. La valeur optimale est alors $w(M) = 80$. Elle s'obtient pour $w(M_{\varphi_1}) = 4$ (c'est-à-dire $(M_{\varphi_1} = I_4)$), $w(M_{\varphi_2}) = w(M_{\varphi_4}) = 5$ et $w(M_{\varphi_3}) = 6$.

Les matrices MDS dyadiques ainsi obtenues ont des propriétés assez particulières

En dessous des résultats surprenants qu'on a pu obtenir :

— Les deux matrices de poids 5 sont toujours les transposées l'une de l'autre.

— La matrice de poids 6 est toujours symétriques.

— Les matrices dyadiques obtenues en permutant les endomorphismes φ_i sont toutes MDS.

En revanche, il faut bien noter que ces propriétés sont en général fausses si on ne pose pas la contrainte du poids minimal.

A permutation près des φ_i, il y a 12 matrices MDS dyadiques de poids 80.

On donne un exemple de ce résultat.

Exemple 16.

$$\varphi_1 = Id,\ M_{\varphi_2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},\ M_{\varphi_3} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix},\ M_{\varphi_4} = M_{\varphi_2}^T.$$

On note que l'ordre de φ_2 est 6, ce qui montre que cet exemple ne peut pas être construit à partir du corps fini $\mathbb{F}_{2^4}$. De plus φ_2 et φ_3 ne sont pas commutatifs.

8.7.4 Cas circulant pour $m = 4$ et $k = 4$

Dans le cas des matrices circulantes $\mathcal{M} = circ(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, le poids minimal est 76. Il s'obtient (à permutation circulaire près) pour $\varphi_1 = \varphi_2 = 1$, $w(M_{\varphi_3}) = 5$ et $w(M_{\varphi_4}) = 6$.

De plus, dans le cas optimal, si $circ(Id, Id, \varphi_3, \varphi_4)$ est MDS, alors $circ(Id, Id, \varphi_4, \varphi_3)$ est aussi MDS.

On obtient dans ce cas 24 matrices MDS circulantes de poids 76.

Exemple 17. $\varphi_1 = \varphi_2 = Id,\ \varphi_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},\ \varphi_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$

Dans cet exemple φ_3 peut être vu comme une matrice de multiplication des éléments primitifs du corps fini $\mathbb{F}_{2^4}$. De plus $\varphi_4 = \varphi_3^{13}$. On peut dire que cet exemple est dérivé des matrices MDS sur $\mathbb{F}_{2^4}$. Ces deux remarques restent vrais pour les 24 matrices MDS circulantes de poids 76.

8.7.5 Cas structuré pour $m = 8$ et $k = 4$

À la section 8.6.1, on a effectué une recherche exhaustive de matrices MDS structurées avec un poids de Hamming minimal sur les corps finis. En permutant les φ_i de la matrice $dyad(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, on parvient à avoir deux matrices MDS dyadiques de poids 188 et deux matrices MDS circulantes de poids 164. Cette différence de poids est due au fait que dans le cas circulaire il est possible de choisir $\varphi_1 = \varphi_2 = 1$. Ces résultats peuvent être comparés avec ceux de l'AES. Le poids de Hamming de la matrice MixColumns est 192, bien que l'architecture de l'AES donne la priorité à l'implémentation logicielle.

En revanche la recherche exhaustive des matrices sur le groupe linéaire $GL(8, 2)$ nous a été impossible, même pour des matrices de petits poids, à cause de son cardinal. On a essayé de trouver d'une manière aléatoire des matrices de poids faible, mais cela ne nous a pas permis de trouver des matrices intéressantes.

On peut aussi utiliser la méthode itérative décrite au paragraphe 7.2.3 permettant de construire des matrices de taille $k = 4$ sur des blocs de 8 bits à partir d'une matrice de taille $k = 4$ sur des blocs de 4 bits.

Toutefois, on peut construire de maniére générique des matrices MDS sur le corps fini $\mathbb{F}_{2^{2m}}$ à partir des matrices MDS sur le corps fini $\mathbb{F}_{2^m}$ de la manière suivante :

Supposons que $M = (M_{i,j})_{i,j\in[1,\ldots,k]}$ et $M' = (M'_{i,j})_{i,j\in[1,\ldots,k]}$ sont deux matrices m-bloc MDS binaires, de taille $r \times r$, en particulier les $M_{i,j}$ et $M'_{i,j}$ sont des éléments du groupe linéaire $GL(m, 2)$. On pose

$$N_{i,j} = \begin{pmatrix} M_{i,j} & 0 \\ 0 & M'_{i,j} \end{pmatrix} \text{ pour } i, j \in [1, \ldots, k].$$

La matrice $N = (N_{i,j})_{i,j\in[1,r]}$ est une matrice $2m$-bloc MDS binaire de taille $r \times r$.

Dans la pratique, cette construction nous permet de construire des matrices $8 - bloc$ MDS (c'est à dire des matrice de bloc de taille 8), pour $2m = 8$ à partir de matrices $4 - bloc$ MDS, pour $m = 4$.

Comme cas particulier on peut choisir $M = M'$. En employant cette méthode pour les paramètre $m = 4$ et $r = 4$, on peut construire des matrices dyadiques MDS de taille de bloc $m = 8$ et de poids $2 \times 80 = 160$ à partir de l'exemple 16 du paragraphe 8.7.3, de même que des matrices circulantes MDS de taille de bloc $m = 8$ et de poids $2 \times 76 = 154$ à partir de l'exemple 17 du paragraphe 8.7.4.

Exemple 18. *Nous détaillons ici l'exemple 16 correspondant au cas dyadique du paragraphe 8.7.3.*

Soient $M_1 = Id_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$,

$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ *et* $M_4 = M_2^T$.

La matrice dyadique $M = \begin{pmatrix} M_1 & M_2 & M_3 & M_4 \\ M_2 & M_1 & M_4 & M_3 \\ M_3 & M_4 & M_1 & M_2 \\ M_4 & M_3 & M_2 & M_1 \end{pmatrix}$ *est la matrice obtenue à l'exemple 16. C'est une matrice dyadique MDS qui agit sur* $k = 4$ *blocs de taille* $m = 4$. *Elle est de poids de Hamming 80.*

On construit alors la matrice

$$M' = \left(\begin{array}{cc|cc|cc|cc} M_1 & 0 & M_2 & 0 & M_3 & 0 & M_4 & 0 \\ 0 & M_1 & 0 & M_2 & 0 & M_3 & 0 & M_4 \\ \hline M_2 & 0 & M_1 & 0 & M_4 & 0 & M_3 & 0 \\ 0 & M_2 & 0 & M_1 & 0 & M_4 & 0 & M_3 \\ \hline M_3 & 0 & M_4 & 0 & M_1 & 0 & M_1 & 0 \\ 0 & M_3 & 0 & M_4 & 0 & M_1 & 0 & M_2 \\ \hline M_4 & 0 & M_3 & 0 & M_2 & 0 & M_1 & 0 \\ 0 & M_4 & 0 & M_3 & 0 & M_2 & 0 & M_1 \end{array}\right)$$

C'est une matrice MDS dyadique agissant sur $k = 4$ *blocs de taille* $m = 8$. *Son poids de Hamming est* $4 \times 80 = 320$.

8.7.6 Cas $k = 8$

Le fait de construire des matrices MDS de taille $r = 8$, est d'un grand intérêt pour les applications cryptographiques. Cependant on se trouve confronté à deux obstacles majeurs. Le premier obstacle est le fait que la recherche exhaustive porte alors sur un nombre trop important de candidats, il faudrait donc trouver des critères permettant de limiter cette recherche. Le deuxième obstacle est celui du coût du test de MDS, qui peut éventuellement être appliqué sur un nombre limité de candidats, mais ne peut être utilisé dans le cadre d'une recherche exhaustive.

Chapitre 9

Codes GRS et matrices dyadiques

Nous présentons dans ce chapitre une construction effective de matrices de diffusion MDS dyadiques dérivées des codes de Reed-Solomon pour toutes les valeurs de m.

Il existe déjà une méthode de construction des matrices dyadiques en utilisant les matrices de Cauchy [48]. On montrera que ces deux méthodes sont duales l'une de l'autre, et qu'elles conduisent aux mêmes matrices MDS dyadiques.

9.1 Matrices MDS dérivées des codes de Reed Solomon

La famille des codes de Reed Solomon et de Reed Solomon généralisés constitue le principal exemple de construction de codes MDS, notamment [46] [35].

La construction d'un code de Reed Solomon généralisé de longueur $s = 2k \leq 2^m$ et de dimension k sur le corps fini $\mathbb{F}_{2^m}$ permet d'obtenir une matrice de diffusion MDS de taille k sur $\mathcal{F}$.

9.1.1 Codes de Reed Solomon

Les codes de Reed Solomon sont des codes correcteurs d'erreurs MDS basés sur les corps finis, et peuvent être introduit de plusieurs manières. Nous utiliserons la présentation en tant que codes d'évaluation de polynômes. Nous nous limitons aux codes de Reed Solomon en caractéristique 2.

Soit $K = \mathbb{F}_{2^m}$ un corps fini, on considère l'anneau des polynômes $T = K[x]/(X^{2^m} - X)$. Il est bien connue notamment dans [24] que l'anneau T est isomorphe aux applications de K dans lui même. Autrement dit toutes les applications de K dans K sont des applications polynomiales de degré inférieur à 2^m.

On note $P_k = \{P(X) \in T / deg(P(X)) < k\}$ l'ensemble des polynômes de degré inférieur strictement à k. L'ensemble P_k est un K-espace vectoriel de T de dimension k.

Soit $S = (a_1, \ldots, a_s)$ un ensemble ordonné d'éléments distincts de K.

Définition 46. *Le code de Reed Solomon $RS_{k,S}$ de dimension k et de support S, est le code obtenue en évaluant les éléments de P_k sur les éléments de S.*

$$RS_{k,S} = \{(P(a_1), P(a_2), \ldots, P(a_s)) \in K^s | P(X) \in P_k\}.$$

Puisque P_k est un K-sous espace vectoriel et la fonction d'évaluation est K-linéaire, le code $RS_{k,S}$ est K-linéaire.

Tout polynôme non nul de degré strictement inférieur à k a au plus $k-1$ racines. De ce fait, on peut déduire que la distance minimale d'un tel code satisfait $d \leq s - (k+1)$, ainsi ce code est un code MDS et $k + d = s + 1$. En utilisant l'évaluation de la base canonique $(1, X, X^2, \ldots, X^{k-1})$ de P_k, on retrouve la matrice génératrice classique d'un code de Reed Solomon [26] :

$$\mathcal{G}_{k,S} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_s \\ a_1^2 & a_2^2 & \ldots & a_s^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \ldots & a_s^{k-1} \end{pmatrix}$$

9.1.2 Matrice de redondance d'un code RS

Soit C le code de Reed Solomon de paramètres $[2k, k, k+1]$ sur le corps fini $K = \mathbb{F}_{2^m}$. À partir de C on peut obtenir une matrice MDS en construisant sa matrice génératrice $G = (\mathbf{I}_k | \mathbf{M})$ sous la forme systématique, on obtient ainsi une matrice MDS $\mathbf{M}$ sur K.

Étudions la structure de $\mathbf{M}$ en détail.

On pose $\mathbf{M} = (a_{i,j})$. La première ligne de la matrice génératrice systématique du code C est $G_1 = (1, 0, \ldots, 0, a_{1,1}, a_{1,2}, \ldots, a_{1,k})$. Cette ligne correspond à l'évaluation du polynôme :

$$P_1(X) = b_1^{-1} \prod_{i=2}^{k} (X - a_i) \text{ avec } b_1 = \prod_{i=2}^{r} (a_1 - a_i).$$

En effet $deg(P_1(X)) = k - 1 \leq k$, $P_1(a_1) = 1$ et $P_1(a_i) = 0$, pour $i = 2$ à r. On peut déduire alors que $a_{1,i} = P_1(a_{k+i})$.

En suivant le même raisonnement, on obtient :

$$P_i(X) = b_i^{-1} \prod_{j=1, j\neq 0}^{k} (X - a_j) \text{ avec } b_i = \prod_{j=1, j\neq i}^{k} (a_i - a_j) \text{ pour tout } i \in [1, \ldots, k]$$

On a alors $a_{i,j} = P_i(a_{k+j})$, pour tout i et j.

9.1.3 Groupe de permutation des codes RS

L'ensemble des permutations du support d'un code correcteur d'erreur qui laisse ce code globalement invariant forme ce qu'on appelle le groupe de permutations du code [4, 5].

Dans ce paragraphe, on s'intéresse dans un premier temps aux codes de Reed Solomon de taille $s = 2^m$. Dans ce cas, le support S du code contient tous les éléments de K. Un tel code est appelé code de Reed Solomon étendu car il est obtenu à partir du code de Reed Solomon cyclique de longueur $2^m - 1$ en ajoutant un symbole de parité.

On note $AGL(1, K)$ le groupe affine sur K, c'est-à-dire l'ensemble des transformations affines $\sigma_{a,b} : X \to aX + b$, avec $a \in K^*$ et $b \in K$. La transformation $\sigma_{a,b}$ sur le support S, agit de la manière suivante :

Si $S = (a_1, ..., a_s)$, alors $\sigma_{a,b}(S) = (a.a_1 + b, ..., a.a_s + b)$. De même, $\sigma_{a,b}$ agit sur les mots de codes : si $c = (P(a_1), \ldots, P(a_s))$, alors $\sigma_{a,b}(c) = (Q(a_1), \ldots, Q(a_s))$ avec $Q(X) = P(aX + b)$.

Puisque $a \neq 0$, on peut remarquer que $deg(Q(X)) = deg(P(X))$. En conséquence et selon la section 9.1.1, un code de Reed Solomon étendu est invariant sous l'action du groupe affine $AGL(1, K)$.

On peut aussi prouver qu'il n'existe pas d'autre permutation laissant ce code globalement invariant [18].

Dans le cas où $s < 2^m$, et en tenant compte des propriétés précédentes, on peut montrer que $RS_{k,S} = RS_{k,\sigma_{a,b}(S)}$.

Cette dernière propriété liée à la double transitivité du groupe affine permet de fixer de manière arbitraire deux éléments du support.

On peut par exemple toujours supposer que $a_1 = 0$ et $a_2 = 1$, même si le support S est de longueur inférieure à 2^m.

Dans le cas particulier où le support S est en fait un $\mathbb{F}_2$-sous-espace vectoriel V de K, alors le code $RS_{k,S}$ est invariant par les translations $\sigma_b : X \to X + b$, avec $b \in V$.

9.2 Matrices MDS dyadiques

Dans ce paragraphe, nous montrons que, en choisissant un support particulier pour le code de Reed Solomon, la matrice de redondance $\mathbf{M}$ est non seulement MDS, mais aussi dyadique et involutive.

9.2.1 Matrices MDS dyadiques involutives

Soit $r = 2^v$, avec $v \leq m$, et $V \subset K$ un espace vectoriel de dimension v sur $\mathbb{F}_2$. On pose $\mathcal{B} = (\beta_0, \ldots, \beta_{v-1})$ une base de V.

On définit le support $S_{\mathcal{B}} = (a_0, \ldots, a_{r-1})$ de la manière suivante :

$a_0 = 0$, $a_1 = \beta_0$, $a_2 = \beta_1$, $a_3 = \beta_0 + \beta_1$, et plus généralement $a_i = \Sigma_{j=0}^{v-1} i_j \beta_j$ où $i = \Sigma_{j=0}^{v-1} i_j 2^j$ est la décomposition de i en base 2.

On a en particulier $a_{2^j} = \beta_j$.

Par exemple pour $v = 3$, si $\beta = (1, \beta_1, \beta_2)$, alors $S_\beta = (0, 1, \beta_1, 1+\beta_1, \beta_2, 1+\beta_2, \beta_1+\beta_2, 1+\beta_1+\beta_2)$.

Puisque les éléments de S_β sont les éléments de l'espace vectoriel V, alors ce support est invariant par l'action de la translation par n'importe quel élément $b = a_j$ de V.

Le lemme suivant caractérise de telles translations :

Lemme 16. *Si $b = a_j$, alors $\tau_b(a_i) = a_i + a_j = a_{i\oplus j}$, pour tout i, j dans $[0; r-1]$.*

Démonstration. Soit $i = \sum_{t=0}^{v-1} i_t 2^t$ et $j = \sum_{t=0}^{v-1} j_t 2^t$.

Par définition, on a $a_i = \sum_{t=0}^{v-1} i_t \beta_t$ et $a_j = \sum_{t=0}^{v-1} j_t \beta_t$.

Ce qui implique que :

$$a_i + a_j = \sum_{t=0}^{v-1} (i_t + j_t \bmod 2)\beta_t = a_{i\oplus j}.$$

□

Lemme 17. *Soit $\mathcal{P}_i$ la matrice de permutation dyadique de taille k, dont la première ligne est e_i. On a : $S_{\mathcal{B}}\mathcal{P}_i = \tau_{a_i}(S_{\mathcal{B}})$, pour tout i in $[0, \ldots, r-1]$.*

Démonstration. On a $\tau_{a_i}(S_{\mathcal{B}}) = (a_0 + a_i, a_1 + a_i, ..., a_{k-1} + a_i)$. Comme conséquence de la proposition 37 on a $S_{\mathcal{B}}\mathcal{P}_i = (a_{0\oplus i}, a_{1\oplus i}, ...a_{(k-1)\oplus i})$.

L'égalité est alors une conséquence du Lemme 16. □

Le résultat principal de cette section est le théorème suivant :

Théorème 25. *La matrice MDS* $\mathbf{M}$*, obtenue à partir d'un code de Reed Solomon est une matrice dyadique, de plus* $\mathbf{M}$ *est involutive.*

Démonstration.

On sait qu'un code de Reed Solomon est invariant par translation de son support. On considère alors le support S_β, généré par la base $\beta = (b_0, \ldots, b_{v-1})$. Soit $\tau_{b_{v-1}}$ la translation $\tau_{b_{v-1}} : x \mapsto x + b_{v-1}$.

Cette translation appliquée à S_β est la permutation définie par $a_i \mapsto a_{i\oplus 2^{v-1}}$. Ainsi elle permute la première partie du support avec la deuxième :

$$\tau_{b_{v-1}}(S_{\mathcal{B}}) = (a_k, ..., a_{r-1}, a_0, ..., a_{k-1}))$$

avec $r = 2k$.

L'image par τ_{b_v}, de la matrice génératrice $G = (\mathbf{I}_k|\mathbf{M})$ de RS_{k,S_β} est $G' = (\mathbf{M}|\mathbf{I}_k)$. Puisque C est un code MDS, alors $\mathbf{M}$ est inversible. La matrice $(\mathbf{I}_k|\mathbf{M}^{-1})$ est aussi une matrice génératrice de RS_{k,S_β}, ce qui implique que $\mathbf{M} = \mathbf{M}^{-1}$, donc $\mathbf{M}$ est une matrice involutive.

Soit la translation τ_i, avec $i \leq 2^{v-2}$ ($i_{2^{v-1}} = 0$). Une telle valeur de i sous cette condition, ne définit pas seulement la matrice de permutation $\mathcal{P}_i$ de taille

$2^v \times 2^v$, mais aussi la permutation similaire $\mathcal{P}'_i$ de taille $2^{v-1} \times 2^{v-1}$. De plus on a la relation $\mathcal{P}_i = I_2 \otimes \mathcal{P}'_i = \begin{pmatrix} \mathcal{P}'_i & 0 \\ 0 & \mathcal{P}'_i \end{pmatrix}$.

L'image de la matrice génératrice $G = (\mathbf{I}_k|\mathbf{M})$ de RS_{k,S_β} par τ_i est $G' = (\mathbf{I}_k|\mathbf{M})\mathcal{P}_i = (\mathcal{P}'_i|\mathbf{M}\mathcal{P}'_i)$. En conséquence, $(\mathbf{I}_k|\mathcal{P}'_i\mathbf{M}\mathcal{P}'_i)$ est une autre matrice génératrice sous la forme systématique pour ce code.

Ainsi $\mathcal{P}'_i\mathbf{M}\mathcal{P}'_i = \mathbf{M}$ pour tout $i \in [0; k-1]$, et en tenant compte du Corollaire 36, on peut dire que $\mathbf{M}$ est une matrice dyadique, ce qui complète la démonstration. □

9.2.2 Matrices MDS dyadiques et codes GRS

Les codes de Reed Solomon généralisés sont dérivés des codes de Reed Solomon en utilisant une multiplication scalaire.

Soit $\mathcal{S} = (a_1, \ldots, a_s)$ un ensemble ordonné d'éléments distincts de K, et $\Lambda = (\lambda_1, ..., \lambda_s) \in K^*$ un ensemble ordonné de scalaires non nuls. On note par D_Λ la matrice de taille $s \times s$, dont la diagonale est Λ.

Définition 47. *Le code de Reed Solomon généralisé de dimension k, scalaire λ et support $\mathcal{S}$, est l'image du code de Reed Solomon $RS_{k,\lambda,\mathcal{S}}$ par la multiplication scalaire par D_λ :*

$$GRS_{k,\mathcal{S}} = \{(\lambda_1 P(a_1), ..., \lambda_s P(a_s)) \in K^s \mid P(X) \in \mathcal{P}_k\}.$$

Selon la démonstration du théorème 25 et du corollaire 36, un code de Reed Solomon généralisé permet de construire une matrice MDS dyadiques si son groupe de permutation contient les permutations $\mathcal{P}_i$ pour tout $i < 2^{v-1}$.

La solution consiste à choisir deux constantes non nulles λ et μ et à construire le support de $\mathcal{S}$ à partir d'un support de la forme $\mathcal{S}_\mathcal{B}$ en multipliant la première moitié du support par λ et la deuxième par μ. D'un point de vue matriciel, on pose $D_\Lambda = \begin{pmatrix} \lambda\mathbf{I}_k & 0 \\ 0 & \mu\mathbf{I}_k \end{pmatrix}$, $\lambda, \mu \in K^*$, $\Lambda = (\lambda, ..., \lambda, \mu, ..., \mu)$.

Si $(\mathbf{I}|\mathbf{M})$ est la matrice génératrice sous forme systématique du code de Reed Solomon $RS(k, \mathcal{S}_\mathcal{B})$, alors la matrice génératrice sous forme systématique du code de Reed Solomon généralisé $GRS(k, \Lambda, \mathcal{S}_\mathcal{B})$ est $(\mathbf{I}|\lambda^{-1}\mu\mathbf{M})$.

En utilisant quelques résultats techniques sur les groupes d'automorphisme des codes de Reed Solomon généralisés [10, 18], et en cherchant les sous-groupes du groupe linéaire $AGL(2, 2^m)$ qui sont isomorphes à $(\mathbb{F}_2, +)^{2^{v-1}}$, on peut montrer qu'il n'est pas possible de construire d'autres matrices MDS dyadiques à partir des codes de Reed Solomon généralisés que celles que l'on vient de décrire.

Exemple 19. *Dans le but de construire une bonne matrice MDS de paramètres $m = 4$ et $r = 8$, on va utilisé notre construction pour les matrices dyadiques sur le corps fini $K = \mathbb{F}_{2^4}$.*

On pose $K = \mathbb{F}_{2^4} = \mathbb{F}_2(a)$ avec $a = X^4 + X + 1$. La base $\mathcal{B} = (1, a, a^2, a^3)$ est la base polynomial standard de $\mathbb{F}_{16}$. Ce qui permet d'avoir une matrice MDS de taille 8 :

$$\mathbf{M}_8 = \begin{pmatrix} a^{12} & a & a^6 & a^8 & a^9 & a^2 & a^4 & a^3 \\ a & a^{12} & a^8 & a^6 & a^2 & a^9 & a^3 & a^4 \\ a^6 & a^8 & a^{12} & a & a^4 & a^3 & a^9 & a^2 \\ a^8 & a^6 & a & a^{12} & a^3 & a^4 & a^2 & a^9 \\ a^9 & a^2 & a^4 & a^3 & a^{12} & a & a^6 & a^8 \\ a^2 & a^9 & a^3 & a^4 & a & a^{12} & a^8 & a^6 \\ a^4 & a^3 & a^9 & a^2 & a^6 & a^8 & a^{12} & a \\ a^3 & a^4 & a^2 & a^9 & a^8 & a^6 & a & a^{12} \end{pmatrix}$$

9.2.3 Comparaison avec les codes de Cauchy

Il existe déjà une méthode de construction de matrices MDS dyadiques pour les applications cryptographiques. Cette méthode est basée sur les matrices de Cauchy, a été introduite dans [48], et utilisée en cryptographie symétrique en particulier dans [6, 33, 34, 42].

Définition 48. *Soient $x = (x_0, ..., x_{k-1})$ et $y = (y_0, ..., y_{k-1})$, deux k-uplets d'élément tous distincts de K (c'est-à-dire $x_i \neq x_j$, $y_i \neq y_j$, $x_i \neq y_i$ et $x_i \neq y_j$ pour tout $i \neq j$). La matrice de Cauchy associée aux k-uplets de x et y est définie par $\mathbf{M}_{x,y} = \left(\frac{1}{x_i - y_j}\right)$.*

Dans [48], les auteurs introduisent des conditions sur les x_i et les y_i, pour obtenir des matrices dyadiques. Ces conditions correspondent en fait à l'invariance par les matrices de permutation $\mathcal{P}_i$.

Dans l'article [18], théorème 2, Arne Dür montre que les matrices de redondance des codes GRS sont des matrices de Cauchy. La correspondance explicite entre les coefficients de x et y et les paramètres du code GRS est décrite dans l'article.

Dans [36], Roth et Seroussi ont montré que toute matrice de Cauchy correspond à une matrice de redondance d'un code GRS.

Ceci permet de démontrer que la construction utilisant les codes de Cauchy introduite dans [48] et celle dérivée des codes de Reed Solomon sont équivalentes et produisent les mêmes matrices de diffusion MDS dyadiques.

9.3 Résultats complémentaires

Dans cette section, nous montrons d'abord qu'une construction à partir des codes GRS ne permet pas d'obtenir des matrices MDS circulantes. Nous montrons ensuite que, lorsque la taille de la matrice est maximale, c'est-à-dire $k = 2^{m-1}$, la construction dyadique à partir des codes de Reed Solomon ne donne qu'une seule matrice MDS à équivalence près.

9.3.1 Codes GRS et matrices MDS circulantes

Pour construire des matrices MDS circulantes, il faut un code dit doublement circulant, c'est-à-dire par permutation circulaire simultanée des k premières coordonnées et des k dernières.

Pour montrer qu'il n'est pas possible de construire des matrices MDS circulantes correspondants à un code GRS, if faut montrer qu'aucun groupe de permutations d'un code GRS ne contient une permutation doublement circulante, c'est-à-dire une permutation constituée de 2 cycles, de même longueur k agissant sur $2k$ éléments.

En utilisant les résultats sur les groupes des automorphisme des codes de Reed Solomon généralisés [10, 18], cette permutation doublement circulante doit être un élément du groupe affine $AGL(m, 2)$, ou bien au moins la restriction de l'action d'un élément de $AGL(m, 2)$ au support $S \subset K$.

Le groupe $AGL(m, 2)$ est de semi-produit direct du groupe des translations $\{\tau_b : x \mapsto x + b \mid b \in K\} \simeq (K, +)$ et du groupe cyclique $\{\sigma_a : x \mapsto ax \mid a \in K^*\} \simeq (K^*, \times)$.

On note que l'ordre de $(K^*, \times)$ est : $2^m - 1$, il ne contient donc pas d'éléments d'ordre pair. Les éléments de $(K, +)$ sont d'ordre 2, le seul cas possible est $k = 2$, ce qui correspond au cas où une matrice circulante est une matrice dyadique.

En conséquence les matrices MDS circulantes ne peuvent pas être dérivées des codes de Reed Solomon généralisés. À notre connaissance il n'y a pas de construction générique de matrices MDS circulantes.

9.3.2 Existe-t'il d'autres matrices MDS dyadiques ?

Une question naturelle est de savoir s'il existe d'autres matrices MDS dyadiques que celles dérivées des codes de Reed-Solomon. Dans le cas général, à savoir les matrices à coefficients dans $\mathcal{L}$, la réponse est oui. Nous montrons que, pour $k = 4$ et $4 \leq m \leq 8$, il existe d'autres matrices MDS dyadiques sur le corps fini $\mathbb{F}_{2^m}$ que celles obtenues à partir de la construction des codes de Reed Solomon.

On note par $\mathcal{D}_\alpha$ la matrice dyadiques $\mathcal{D}_\alpha = \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix}$, de déterminant 1 sur $\mathbb{F}_{2^m}^*$, et tel que $\alpha \notin \{0, 1\}$.

Cas $k = 2$.

Soit $\mathcal{D} = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$ une matrice dyadique de taille 2×2 sur le corps fini $\mathbb{F}_{2^m}$. On vérifie facilement que $\mathcal{D}$ est MDS et de déterminant 1 si et seulement si $\alpha \notin \{0, 1\}$ et $\beta = \alpha + 1$.

Proposition 45. *On suppose $\alpha \notin \{0, 1\}$. La matrice MDS dyadique construite à partir de la base $\mathcal{B} = (1, \alpha)$ est $\mathcal{D}_\alpha = \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix}$.*

En conséquence toutes les matrices MDS dyadiques de taille 4 *sur* $\mathbb{F}_{2^m}$ *sont obtenues par la construction GRS.*

Démonstration. Le support correspondant à la base $\mathcal{B}$ est $\mathcal{S}_{\mathcal{B}} = (0, 1, \alpha, \alpha+1)$. La matrice génératrice du code de Reed Solomon correspondante est alors

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha+1 \end{pmatrix}.$$

Si on met cette matrice sous forme systématique, la matrice de redondance obtenue est bien la matrice $\mathcal{D}$ cherchée. □

Cas $k = 4$**.**

Le lemme suivant caractérise la forme des matrices MDS dyadiques de taille 4 et de déterminant 1.

Lemme 18. *Si* $\mathcal{D}$ *est une matrice MDS dyadique de taille 4 sur* $\mathbb{F}_{2^m}$ *et de déterminants 1, alors il existe des éléments* α*,* β *et* λ *de* $\mathbb{F}_{2^m}$ *tels que*

$$\mathcal{D} = \begin{pmatrix} \lambda\mathcal{D}_\alpha & (\lambda+1)\mathcal{D}_\beta \\ (\lambda+1)\mathcal{D}_\beta & \lambda\mathcal{D}_\alpha \end{pmatrix}$$

De plus, ces éléments sont uniques, α*,* β *et* λ *sont distincts de 0 et 1,* $\alpha \neq \beta$*,* $\alpha \neq \beta + 1$

Démonstration. Il suffit de regarder les 2 sous-matrices M_1 et M_2 telles que $\mathcal{D} = \begin{pmatrix} M_1 & M_2 \\ M_2 & M_1 \end{pmatrix}$. Si λ et μ sont les éléments de $\mathbb{F}_{2^m}$ tels que $\lambda^2 = det(M_1)$ et $\mu^2 = det(M_2)$, les matrices $\lambda^{-1}M_1$ et $\mu^{-1}M_2$ sont des matrices MDS dyadiques de taille 2 et déterminant 1. D'après la proposition 45, elles sont respectivement de la forme $\mathcal{D}_\alpha$ et $\mathcal{D}_\beta$.

La propriété $\mu = \lambda + 1$ provient de la contrainte $Det(\mathcal{D}) = 1$. Les autres conditions s'obtiennent en regardant certains sous-déterminants 2×2 de $\mathcal{D}$ qui ne sont pas nuls. □

Il faut noter que les conditions du lemme précédent ne sont que des conditions nécessaires. Les contraintes sur les sous-déterminants non nuls sont plus complètes, mais nous n'avons pas trouvé de formulation générique valable pour tout m.

La proposition suivante décrit les matrices MDS dyadiques construites à partir de codes de Reed Solomon.

Proposition 46. *La matrice MDS dyadique dérivée des codes de Reed Solomon et construite à partir de la base* $\mathcal{B} = (1, \alpha+\beta, \beta)$ *est la matrice* $\mathcal{D}_{\mathcal{B}}$ *suivante :*

$$\mathcal{D} = \begin{pmatrix} \lambda\mathcal{D}_\alpha & (\lambda+1)\mathcal{D}_\beta \\ (\lambda+1)\mathcal{D}_\beta & \lambda\mathcal{D}_\alpha \end{pmatrix} \quad avec \quad \lambda = \frac{\alpha^2+\alpha}{(\alpha+\beta)^2+(\alpha+\beta)}.$$

Démonstration. La démonstration est une vérification directe, bien qu'un peu technique, en utilisant la forme de la matrice de redondance d'un code de Reed Solomon décrite au paragraphe 9.1.2. □

Corollaire 7. *Pour $4 \leq m \leq 8$, il existe des matrices MDS dyadiques de taille 4×4 sur $\mathbb{F}_{2^m}$ qui ne sont pas dérivées des codes de Reed Solomon.*

Démonstration. Au paragraphe 8.6.1, nous avons vérifié que, pour $4 \leq m \leq 8$, il y a exactement $(2^m-1)(2^m-2)(2^m-4)(2^m-7)$ matrices MDS dyadiques sur $\mathbb{F}_{2^m}$ de taille 4. Il y en a donc $(2^m-2)(2^m-4)(2^m-7)$ de déterminant 1. La proposition précédente montre que l'on peut en obtenir $(2^m-2)(2^m-4)$ à partir de la construction des codes de Reed Solomon. □

9.3.3 Unicité de la construction GRS pour $k = 2^{m-1}$

Dans cette section, nous considérons le cas particulier $k = 2^{m-1}$, c'est-à-dire les codes de longueur $s = 2k = 2^m$. Dans ce cas $\mathcal{B}$ est de taille m et est donc une base de K sur $\mathbb{F}_2$. Le support $\mathcal{S}_{\mathcal{B}}$ est constitué de tous les éléments de K.

On considère donc une matrice MDS dyadique $\mathbf{M}$ construite à partir d'un code de Reed Solomon étendu, de support $\mathcal{S}_{\mathcal{B}}$ dérivé d'une certaine base $\mathcal{B}$ fixée de K sur $\mathbb{F}_2$.

On pose $\mathbf{M} = (a_{i,j})_{0 \leq i,j < k}$ et $L_{\mathcal{B}} = (a_{0,0}, ..., a_{k-1,k-1})$. On a donc $\mathbf{M} = dyad(L_{\mathcal{B}})$.

Nous pouvons maintenant énoncer le résultat de ce paragraphe :

Théorème 26. *L'ensemble $L_{\mathcal{B}}$ ne dépend pas du choix de la base $\mathcal{B}$ choisie.*

Démonstration. Soit V, un hyperplan généré par les éléments de $\mathcal{B}$, sauf le dernier que l'on note b_m. Autrement dit $V = \langle b_1, ...b_{m-1} \rangle$. La première moitié du support $S_{\mathcal{B}}$ est composée des éléments de V, et la seconde partie est $b_m + V$, en respectant l'ordre de V. On note que $K = V \cup (b_m + V)$.

On pose

$$P_V = \prod_{u \in V} (X - u) = \prod_{i=1}^{r} (X - a_i).$$

Puisque V est un espace vectoriel, en utilisant la théorie des polynômes de permutation et celle des polynômes linéarisés [24], chap. 7, on sait que $P(X)$ est un polynôme linéarisé $P(X) = \sum_{j=0}^{m-2} \alpha_j X^{2^j}$. Pour simplifier les notations, on pose également $a_i = a_{0,i}$.

De plus $P(X)$ est $\mathbb{F}_2$-linéaire : $P(x+y) = P(x) + P(y)$.
On pose $Q_1(X) = X(X - b_1)$, puis, par récurrence sur i,

$$Q_{i+1}(X) = Q_i(X)(Q_i(X) - Q_i(b_{i+1})).$$

Les polynômes $Q_i(X)$ sont linéarisés de degré 2^i, et ils ont pour racines l'espace vectoriel engendré par $(b_1, \ldots, b_i)$. Alors $Q_{m-1}(X)$ est un multiple de $P_V(X)$.

En utilisant les résultats présentés dans la section 9.1, on pose :

$$P_{0,V}(X) = \alpha^{-1} P_V(X)/X = \alpha^{-1} \prod_{u \in V^*} (X - u), \text{ avec } \alpha = \prod_{u \in V^*} u.$$

On rappelle que $a_{i,j}$ est le coefficient de la i-ème ligne et de la j-ème colonne de $\mathbf{M}$, et a_i le i-ème élément du support $L_{\mathcal{B}}$. On a $a_{0,j} = P_{0,V}(a_{j+r})$ pour j allant de 0 à $r-1$.

On peut déduire que

$$L_{\mathcal{B}} = \{\alpha^{-1} \prod_{u \in V^*} (u' - u) \mid u' \notin V\}.$$

Ainsi par construction, $P_{0,V}(0) = 1$ et $P_{0,V}(0) = 0$, pour tout u dans V^*, l'image de K par $P_{0,V}(X)$ est

$$P_{0,V}(K) = L_{\mathcal{B}} \cup \{0,1\} = \{\alpha^{-1} \prod_{u \in V^*} (u' - u) \mid u' \in K\}.$$

À ce stade de la démonstration on considère une autre base $\mathcal{B}'$ et un autre hyperplan V' généré par les $m-1$ premiers éléments de $\mathcal{B}'$. On pose $\alpha' = \prod_{u' \in V'^*} u'$, et Soit l l'isomorphisme linéaire tel que $l(b'_i) = b_i$ pour i allant de 1 à m. Ainsi il est claire que $l(V') = V$.

Pour achever cette démonstration on a besoin du lemme suivant :

Lemme 19. *En tenant en compte des notations précédentes, on a l'égalité*

$$P_{V'}(X) = \prod_{u' \in V'} (X - u') \equiv (\alpha'/\alpha) P_V(\ell(X)) \pmod{X^{2^m} - X}.$$

Démonstration.

On commence par remarquer que, si l est une application linéaire, alors $P_V(l(X))$ est un polynôme linéarisé. Puisque son noyau contient V', alors son degré est au moins 2^{m-1}, qui est le degré maximal d'un polynôme linéarisé (calculé modulo $X^{2m} - X$). Alors $P_{V'}(X)$ et $P_V(l(X))$ sont égaux à un scalaire près.

En évaluant $P_{V'}(X)/X$ et $P_V(\ell(X))/X$ pour 0, on obtient α' et α respectivement, alors $P_{V'}(X) = (\alpha'/\alpha) P_V(\ell(X))$. □

De même que précédemment, on a :

$$P_{0,V'}(K) = L_{\mathcal{B}'} \cup \{0,1\} = \{\alpha'^{-1}(\alpha'/\alpha) \prod_{u \in V^*} (\ell(u') - u) \mid u' \in K\}.$$

Ainsi l est bijective sur K, et on peut conclure que :

$$P_{0,V'}(K) = L_{\mathcal{B}} \cup \{0,1\} = \{\alpha^{-1} \prod_{u \in V^*} (u' - u) \mid u' \in K\} = P_{0,V}(K).$$

De plus l'ensemble :

$$P_{0,V}(K) = L_{\mathcal{B}} \cup \{0,1\} = L_{\mathcal{B}'} \cup \{0,1\}$$

contient $2^{m-1}+1$ ou $2^{m-1}+2$ éléments, selon que 1 est dans $L_{\mathcal{B}}$ ou non. Si 1 est déjà dans $L_{\mathcal{B}}$, il suffit de supprimer 0 de $P_{0,V}(K)$ pour obtenir $L_{\mathcal{B}}$ et $L_{B'}$. Si 1 n'est pas dans $L_{\mathcal{B}}$, Alors on doit supprimer 0 et 1 de $P_{0,V}(K)$ pour obtenir $L_{\mathcal{B}}$ et $L_{\mathcal{B}'}$. Dans tous les cas $L_{\mathcal{B}} = L_{\mathcal{B}'}$. □

Conclusion et perspectives

Cette thèse présente une étude de l'application des codes correcteurs d'erreurs en cryptographie. Plus précisément elle explore les codes MDS additifs systématiques dans le but de construire de bonnes matrices de diffusion pour le chiffrement par bloc. Les contributions majeures de cette thèse peuvent être axées sur trois parties. Une première qui porte sur une étude des codes sur le quotient fini d'anneaux de polynômes $\mathcal{A} = \mathbb{F}[x]/f(x)$, où $f(x)$ est un polynôme unitaire sans facteur carré, ces codes sont une généralisation des codes quasi-cycliques. En employant la division euclidienne on a pu donner une matrice génératrice canonique et ainsi généraliser le travail de K. Lally et P. Fitzpatrick dans [23] et examiner le lien entre la dualité sur $\mathcal{A}$ et la dualité binaire de ces codes.

Dans [29] C. Martinez-Pérez et W. Willems ont montré que certaines sous-classes des codes quasi-cycliques sont asymptotiquement bons. La question qui se pose naturellement est "Les $\mathcal{A}$-codes" atteignent-ils la borne de Gilbert-Varshamov ?

Il serait aussi intéressant d'étendre notre étude au cas où le polynôme $f(x)$ a des facteurs carrés. Si $f(x) = f_1(x)^r$, $\mathcal{A}$ est alors un anneau local et principal, et par la suite un anneau de chaînes finis. Une étude des codes sur ces anneaux est a été faite par K. Guenda et T. Aaron Gulliver dans [19].

La deuxième contribution est une étude des codes en bloc additifs systématiques sur des m-uplets binaires, La matrice génératrice de ces codes dont les coefficients sont dans l'anneau $\mathcal{L}$ des endomorphismes de $\mathbb{F}_2^m$ nous a inspiré pour définir et étudier les codes sur $\mathcal{L}$. Nous avons en particulier mis en évidence la correspondance entre un code sous-module à gauche de $\mathcal{L}$ et un code additif sur $\mathbb{F}_2^m$.

La troisième contribution utilise cette étude des codes additifs dans le but d'explorer les matrices MDS de diffusion avec de bonnes propriétés de symétrie pour les applications cryptographiques. Cette exploration est en particulier faite sur des matrices circulantes est dyadiques, ce qui nous a permis de construire des matrices MDS dyadiques de grande taille à partir de matrices de petite taille sur le groupe linéaire $GL(m, 2)$. Enfin on a pu donner quelques résultats théoriques et pratiques efficaces pour les implémentations machine.

L'utilisation durant cette thèse des codes correcteurs d'erreurs sur différentes structures, à savoir le quotient d'anneau de polynômes $\mathbb{F}[x]/f(x)$, le groupe additif $(\mathbb{F}_2^m, +)$ et en fin l'anneau des endomorphisme de $\mathbb{F}_2^m$, nous a permis de déterminer les structures sur lesquelles il serait intéressant de chercher et de construire de bonnes matrices MDS pour la phase de diffusion

linéaire des chiffrements par bloc. En particulier, on a pu constater que le nombre de matrices MDS construite à partir de l'anneau des endomorphismes de $\mathbb{F}_2^m$ est plus grand que le nombre de matrices MDS de diffusion pouvant être construite sur les corps finis. Bien que la famille des matrices circulantes donne de bons résultats pour l'implémentation des matrices MDS de diffusion, la famille des matrices dyadiques apporte deux grands avantages, le premier est le fait qu'il est possible de construire des matrices involutives dyadiques, qui sont de grands intérêt pour le processus de décryptage, et le deuxième est le fait qu'il existe une méthode théorique de construction des matrices MDS. En revanche il nous a pas été possible d'avoir des résultats expérimentales pour $k = 8$. Ainsi il est de grand intérêt en cryptographie de trouver d'autres méthodes pour pouvoir construire des matrices MDS dyadiques de taille $k = 8$.

Bibliographie

[1] Michael Francis Atiyah et I. G. MacDonald : *Introduction to commutative algebra*. Addison-Wesley-Longman, 1969.

[2] Daniel Augot et Matthieu Finiasz : Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. *In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 1551–1555. IEEE, 2013.

[3] Daniel Augot et Matthieu Finiasz : Direct construction of recursive MDS diffusion layers using shortened BCH codes. *In* Carlos Cid et Christian Rechberger, éditeurs : *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 de *Lecture Notes in Computer Science*, pages 3–17. Springer, 2015.

[4] Robert F. Bailey : Permutation groups, error-correcting codes and uncoverings. *Thèse de l'Université de Londre*, 2005.

[5] Robert F. Bailey : Error-correcting codes from permutation groups. *Discrete Mathematics*, 309(13):4253–4265, 2009.

[6] Paulo S. L. M. Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen et Elmar Tischhauser : Whirlwind : a new cryptographic hash function. *Des. Codes Cryptography*, 56(2-3):141–162, 2010.

[7] Thierry P. Berger : Construction of recursive MDS diffusion layers from gabidulin codes. *In* Goutam Paul et Serge Vaudenay, éditeurs : *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*, volume 8250 de *Lecture Notes in Computer Science*, pages 274–285. Springer, 2013.

[8] Thierry P. Berger et Nora El Amrani : Codes over finite quotients of polynomial rings. *Finite Fields and Their Applications*, 25:165–181, 2014.

[9] Thierry P. Berger et Nora El Amrani : Codes over $\mathrm{L}(\mathrm{GF}(2)^m, \mathrm{GF}(2)^m)$, MDS diffusion matrices and cryptographic applications. *In* Said El Hajji, Abderrahmane Nitaj, Claude Carlet et El Mamoun Souidi, éditeurs : *Codes, Cryptology, and Information Security - First International Conference, C2SI 2015, Rabat, Morocco, May 26-28, 2015, Proceedings - In Honor of Thierry Berger*, volume 9084 de *Lecture Notes in Computer Science*, pages 197–214. Springer, 2015.

[10] Thierry P. Berger et Pascale Charpin : The permutation group of affine-invariant extended cyclic codes. *IEEE Transactions on Information Theory*, 42(6):2194–2209, 1996.

[11] Anton Betten et *al.* : Error-correcting linear codes : Classification by isometry and applications. *Springer Science and Business Media*, 18, 2006.

[12] Wieb Bosma, John J. Cannon et Catherine Playoust : The magma algebra system I : the user language. *J. Symb. Comput.*, 24(3/4):235–265, 1997.

[13] Delphine Boucher, Patrick Solé et Felix Ulmer : Skew constacyclic codes over galois rings. *Adv. in Math. of Comm.*, 2(3):273–292, 2008.

[14] Delphine Boucher et Felix Ulmer : Linear codes using skew polynomials with automorphisms and derivations. *Des. Codes Cryptography*, 70(3):405–431, 2014.

[15] Kenneth A. Bush : Orthogonal arrays of index unity. *Annals of Mathematical Statistics*, 13:426–434, 1952.

[16] Joan Daemen et Vincent Rijmen : *The Design of Rijndael : AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.

[17] Whitfield Diffie et Martin E. Hellman : New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[18] Arne Dür : The automorphism groups of Reed-Solomon codes. *J. Comb. Theory, Ser. A*, 44(1):69–82, 1987.

[19] Kenza Guenda et T. Aaron Gulliver : MDS and self-dual codes over rings. *Finite Fields and Their Applications*, 18(6):1061–1075, 2012.

[20] Jian Guo, Thomas Peyrin et Axel Poschmann : The PHOTON family of lightweight hash functions. *In* Phillip Rogaway, éditeur : *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 de *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.

[21] Jian Guo, Thomas Peyrin, Axel Poschmann et Matthew J. B. Robshaw : The LED block cipher. *In* Bart Preneel et Tsuyoshi Takagi, éditeurs : *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 de *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.

[22] Richard Wesley Hamming : Error detecting and error correcting codes. *Bell System technical journal*, 29:147–160, 1964.

[23] Kristine Lally et Patrick Fitzpatrick : Algebraic structure of quasi-cyclic codes. *Discrete Applied Mathematics*, 111(1-2):157–175, 2001.

[24] Rudolf Lidl et Harald Niederreiter : *Finite fields*, volume 20. Cambridge university press, 1997.

[25] San Ling, Harald Niederreiter et Patrick Solé : On the algebraic structure of quasi-cyclic codes IV : repeated roots. *Des. Codes Cryptography*, 38(3):337–361, 2006.

[26] Florence Jessie MacWilliams et Neil James Alexander Sloane : *The theory of Errors Correcting Codes*. Elsevier, 1977.

[27] Jessie MacWilliams : A theorem on the distribution of weights in a systematic code. *Bell System Tech*, 42:79–94, 1963.

[28] Conchita Martínez-Pérez et Wolfgang Willems : Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good. *IEEE Transactions on Information Theory*, 53(11):4302–4308, 2007.

[29] Conchita Martínez-Pérez et Wolfgang Willems : Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good. *IEEE Transactions on Information Theory*, 53(11):4302–4308, 2007.

[30] Robert J. McEliece : A public-key cryptosystem based on algebraic coding theory. *JPL DSN Progress Report*, 42:114–116, 1978.

[31] Harald Niederreiter : Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[32] A Nikseresht : Dual of codes over finite quotients of polynomials rings. *24th Iranian Algebra Seminar*, 2014.

[33] Vincent Rijmen et Paulo S. L. M. Barreto : The anubis block cipher. *In First open NESSIE Workshop, Leuven*, 2000.

[34] Vincent Rijmen et Paulo S. L. M. Barreto : The khazad legacy-level block cipher. *In NESSIE Workshop, Leuven*, volume 97, 2000.

[35] Ron M. Roth et Abraham Lempel : On MDS codes via cauchy matrices. *IEEE Transactions on Information Theory*, 35(6):1314–1319, 1989.

[36] Ron M. Roth et Gadiel Seroussi : On generator matrices of MDS codes. *IEEE Transactions on Information Theory*, 31(6):826–830, 1985.

[37] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala et Pouyan Sepehrdad : Recursive diffusion layers for block ciphers and hash functions. *In* Anne Canteaut, éditeur : *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 de *Lecture Notes in Computer Science*, pages 385–401. Springer, 2012.

[38] Beniamino Segre : Ovals in a finite projective plane. *Canadian Journal of Mathematics*, 7:414–416, 1955.

[39] Gérald E. Séguin : A class of 1-generator quasi-cyclic codes. *IEEE Transactions on Information Theory*, 50(8):1745–1753, 2004.

[40] Gérald E. Séguin : A class of 1-generator quasi-cyclic codes. *IEEE Transactions on Information Theory*, 50(8):1745–1753, 2004.

[41] Claude E. Shannon : A mathematical theory of communication. *Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[42] Taizo SHIRAI, Kyoji SHIBUTANI, Toru AKISHITA, Shiho MORIAI et Tetsu IWATA : The 128-bit blockcipher CLEFIA (extended abstract). *In* Alex BIRYUKOV, éditeur : *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 de *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[43] Siang Meng SIM, Khoongming KHOO, Frédérique E. OGGIER et Thomas PEYRIN : Lightweight MDS involution matrices. *In* Gregor LEANDER, éditeur : *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 de *Lecture Notes in Computer Science*, pages 471–493. Springer, 2015.

[44] Richard C. SINGLETON : Maximum distance q -nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

[45] Joachim VON ZUR GATHEN et Jürgen GERHARD : *Modern Computer Algebra (3. ed.)*. Cambridge University Press, 2013.

[46] Stephen B. WICKER et Vijay K. BHARGAVA : *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.

[47] Shengbao WU, Mingsheng WANG et Wenling WU : Recursive diffusion layers for (lightweight) block ciphers and hash functions. *In* Lars R. KNUDSEN et Huapeng WU, éditeurs : *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 de *Lecture Notes in Computer Science*, pages 355–371. Springer, 2013.

[48] Amr M. YOUSSEF et Stafford E. TAVARES : On the design of linear transformations for substitution permutation encryption networks. *In Selected Areas of Cryptography (SAC'96) : Workshop Record*, pages 40–48, 1997.

Codes additifs et matrices MDS pour la cryptographie

Résumé : Cette thèse porte sur les liens entre les codes correcteurs d'erreurs et les matrices de diffusion linéaires utilisées en cryptographie symétrique. L'objectif est d'étudier les constructions possibles de codes MDS additifs définis sur le groupe $(\mathbb{F}_2^m, +)$ des m-uplets binaires et de minimiser le coût de l'implémentation matérielle ou logicielles de ces matrices de diffusion.
Cette thèse commence par l'étude des codes définis sur un anneau de polynômes du type $\mathbb{F}[x]/f(x)$, qui généralisent les codes quasi-cycliques. Elle se poursuit par l'étude des codes additifs systématiques définis sur $(\mathbb{F}_2^m, +)$ et leur lien avec la diffusion linéaire en cryptographie symétrique. Un point important de la thèse est l'introduction de codes à coefficients dans l'anneau des endomorphismes de $\mathbb{F}_2^m$. Le lien entre les codes qui sont des sous-modules à gauche et les codes additifs est mis en évidence. La dernière partie porte sur l'étude et la construction de matrices de diffusion MDS ayant de bonnes propriétés pour la cryptographie, à savoir les matrices circulantes, les matrices dyadiques, ainsi que les matrices ayant des représentations creuses minimisant leur implémentation.

Mots clés : Codes additifs. Codes MDS. Matrices de diffusion. Cryptographie symétrique. Chiffrement par bloc. Codes sur des anneaux.

Additive codes and MDS matrices codes for the cryptographic applications

Abstract : This PhD Thesis focuses on the links between error correcting codes and diffusion matrices used in cryptography symmetric. The goal is to study the possible construction of additives MDS codes defined over the group $(\mathbb{F}_2^m, +)$ of binary m-tuples and minimize cost of hardware or software implementation of these diffusion matrices.

This thesis begins with the study of codes defined over the polynomial ring $\mathbb{F}[x]/f(x)$, these codes are a generalization of quasi-cyclic codes, and continues with the study of additive systematic codes over $(\mathbb{F}_2^m, +)$ and their relation with linear diffusion on symmetric cryptography. An important point of this thesis is the introduction of codes with coefficients in the ring of endomorphisms of $\mathbb{F}_2^m$. The link between codes which are left-submodules and additive codes have been identified. The last part focuses on the study and construction of efficient diffusion MDS matrices for the cryptographic applications, namely the circulantes matrices, dyadic matrices, and matrices with sparse representation, in ordre to minimize their implementation.

Keywords : Additive codes. MDS codes. Diffusion matrices. Symmetric cryptography. Block cipher. Codes over rings.